

Training "Open Source Tools for CSIRT"

Proof of concept : Build your CSIRT

"Free of License Costs" and with "Return On Investment"



Prof Nabil SAHLI (nabilsahli@gmail.com / n.sahli@ansi.tn)

+ TunCERT :

Eng Mohamed Ben MABROUK (benmabrouk.medali@ansi.tn)

Eng Mondher SMII (smii.mondher@ansi.tn)

+ CSIRT.tn :

Eng Amine RACHED (amine.rached@keystone.tn)

PLAN



I- About Open-Source and CSIRT

CSIRT Infrastructure

II- Network Security Architecture

Eng Mondher SMII

III- Cyber-space Monitoring and Honeynet systems

Eng Nabil HOSNI

Eng Meriem Mahjoubi

CSIRT Activities

IV- CSIRT Process Management systems

- Alert and Warning Process
- Incident Handling Process

Eng Mohamed Ben
MABROUK

V- Forensics and investigation tools

Eng Amine RACHED

*Email of tunCERT and CSIRT.tn
Trainers, in charge of Demos*

TunCERT :

Eng Mohamed Ben MABROUK : benmabrouk.medali@ansi.tn
GLPI, Taranis,

Eng Mondher SMII : smii.mondher@ansi.tn
Pfsense, Surricata ,Oignon, Saher

CSIRT.tn :

Eng Amine RACHED : amine.rached@keystone.tn
CSIRT.TN KIT (FTK, Autopsy, KAPE ...), REM , Kuiper Framework)

MORE, free, TRAINING Take OUT

- ***For inscriptions to the Live Platform or/and Download of Live-DVD : Please send an email to : events@ansi.tn with CC nabilsahli@gmail.com (/n.sahli@ansi.tn) for follows-up***
- ***For inscriptions to Additional Trainings (Installation/Configurations): Please send an email to : events@ansi.tn (with CC nabilsahli@gmail.com), specifying the Tool(s) you are interested with***



**I-
About Open-Source
and
CSIRT**

Cost of Implementation of a CSIRT Infrastructure

- ❑ Equipments (PCs+ Servers + forensics tools)
- ❑ **Software tools :**
 - **License fees**
 - > Recurent **Big annual Maintenance fees**

How to decrease this big « cost center »
+ avoid delays (+...) in CSIRT iservices mplementation,
(escape from « our » painful and long administrative
acquisition procedures)

Be able to More Invest in **Capacity Building**
(**training**, ...) & the funding of CSIRT activities
(awareness campaigns, ...)

CSIRT's Software Needs

Need for a « Strong »
CSIRT Security Architecture

→ **Cardinal** and **qualitative** Completeness of deployed
Solutions

Need for Tools for implementing the CSIRT
process

Need for various and multi-platform
investigation and forensics tools

 **Bigs Budgets** (Expensive licenses,
Recurent cost of maintenance fees,..)

 **SOLUTION = Use of OPEN-SOURCE tools**

~ 0 Licences

Open-Source

"Beautiful world"

- **Free Licences**
 - **Sources Codes disponibles**
- + **Respect of standards**
- + **GUIs and Good Community assistance**
- + **Perinuity** (better than some commercial solutions)
- + **NOW: available optional «Contractual Support» & Training, for "must" solutions (OpenCore)**

FALSE Myths

Open source is "insecure" myth

"it's insecure because everyone can see how it works."

--> No software relies on the obscurity of source code for security. If there was any truth in that, Microsoft Windows would be the most secure OS ever created,

Commercial tools have better "support" myth

--> The "Must" open source tools have "contractual cheap support" (training, assistance, ...)
+ Very Rich and Friendly assistance from the (philanthropic) Community of open-source

Free access to Source codes

Open Source Tools **Can be Customized/Extended**



An enabler for R&D activities

(Other potential Return On Investment)

You are a "Legal provider" of Open source Security solutions



Open Source Tools **Can be installed by the CSIRT on the constituency's infrastructures**

Once you have handled an incident

--> Need to IMMEDIATELY strength the constituency Security

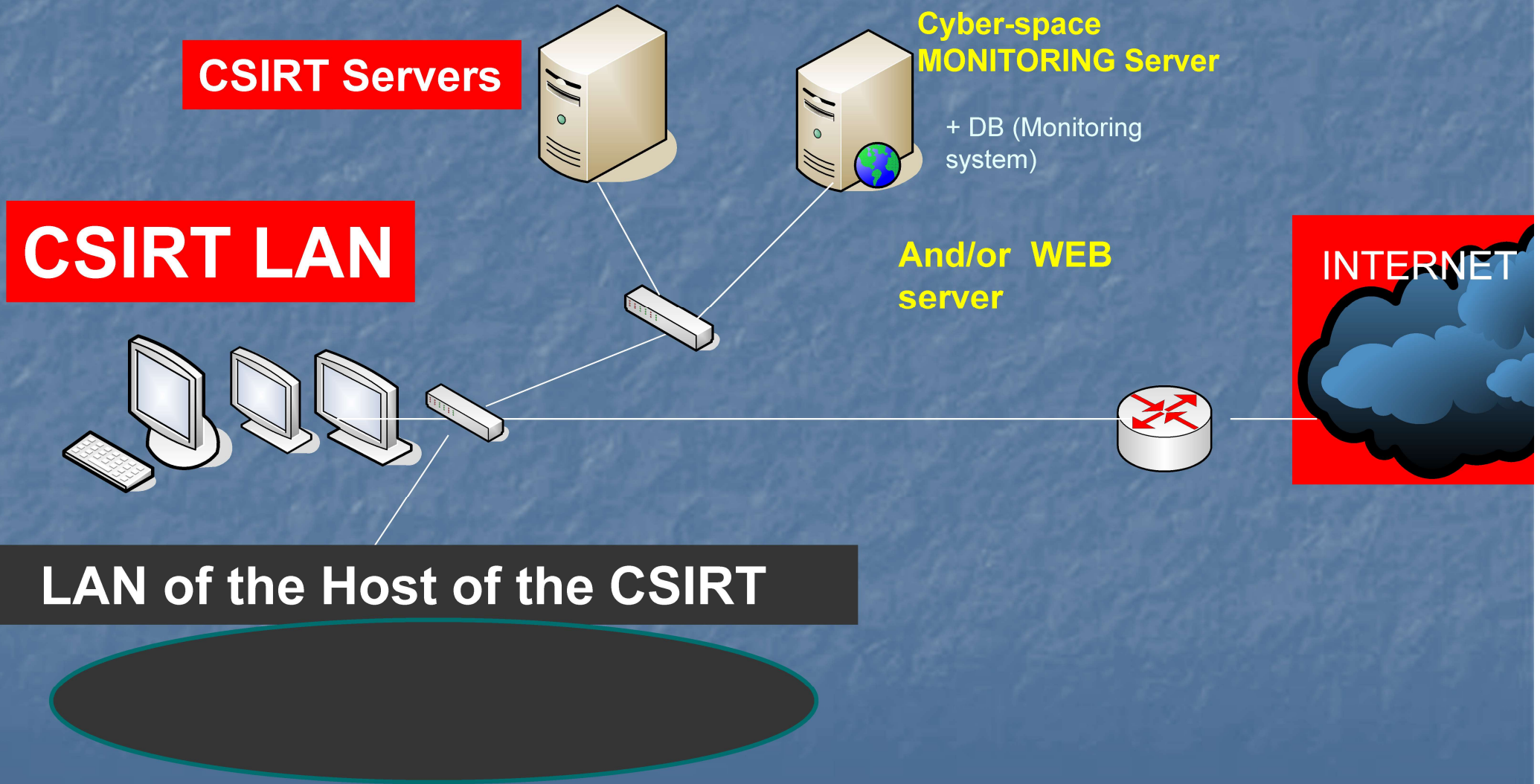
--> Install Open source security Tools

-I-

Building your CSIRT Security Architecture, with Open-Source tools



Network Architecture « generic template »





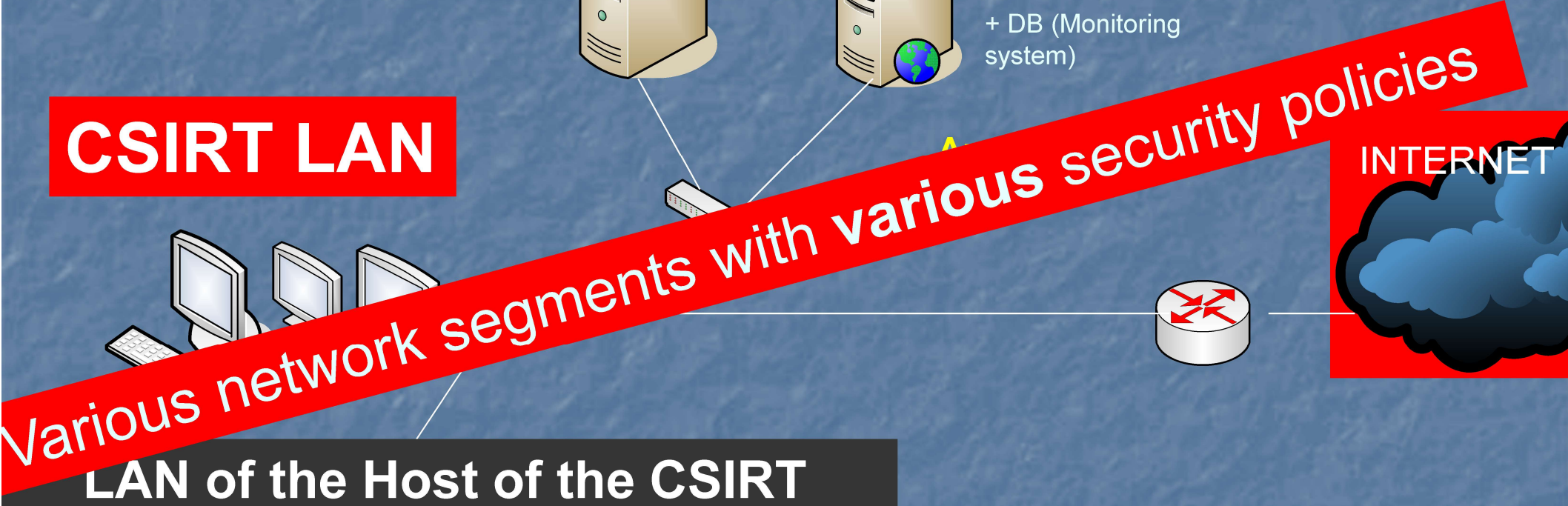
Protection of the Perimeter of your Network

CSIRT Servers

Cyber-space
MONITORING Server

+ DB (Monitoring system)

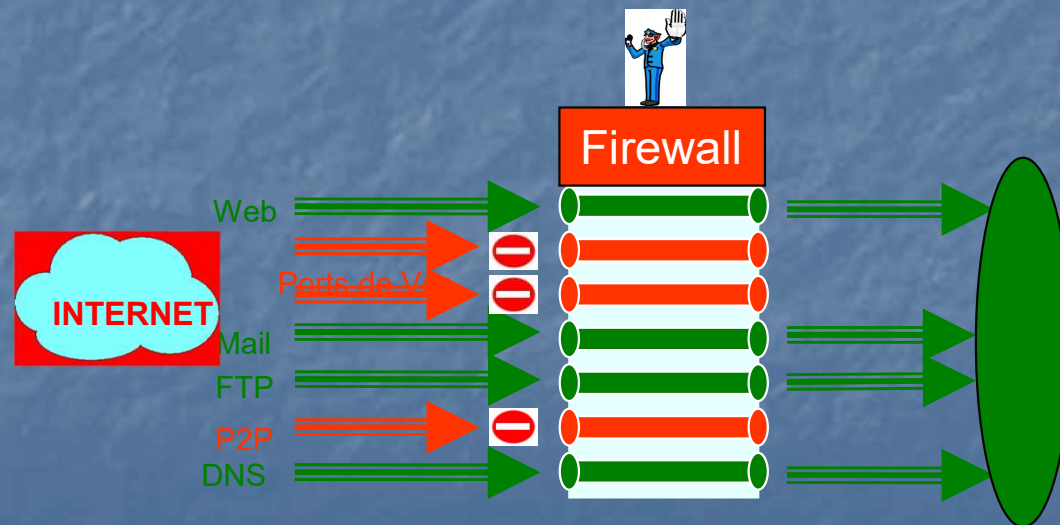
CSIRT LAN



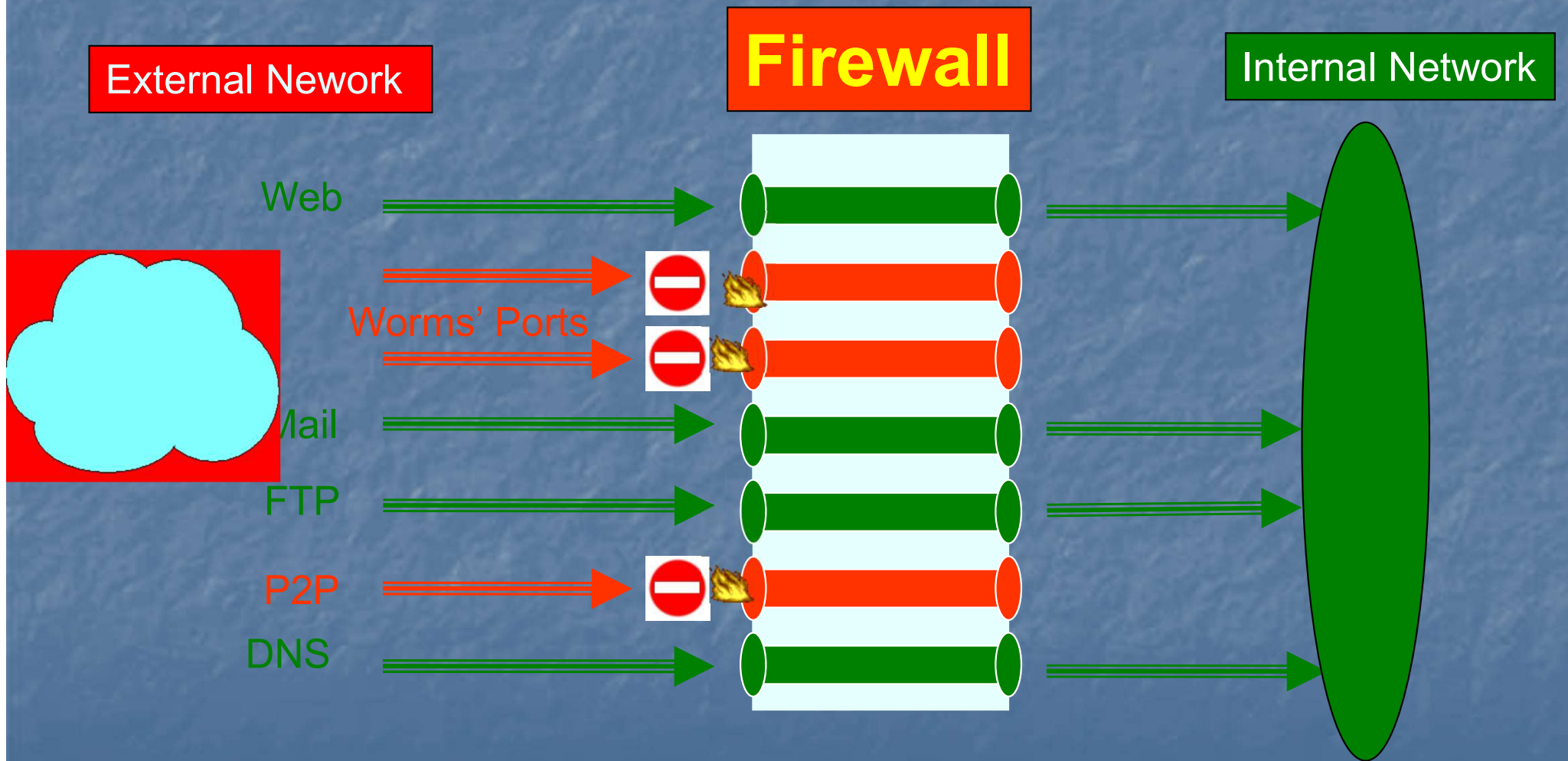
INTERNET

LAN of the Host of the CSIRT

1- FIREWALLING System



Firewall :How it Works



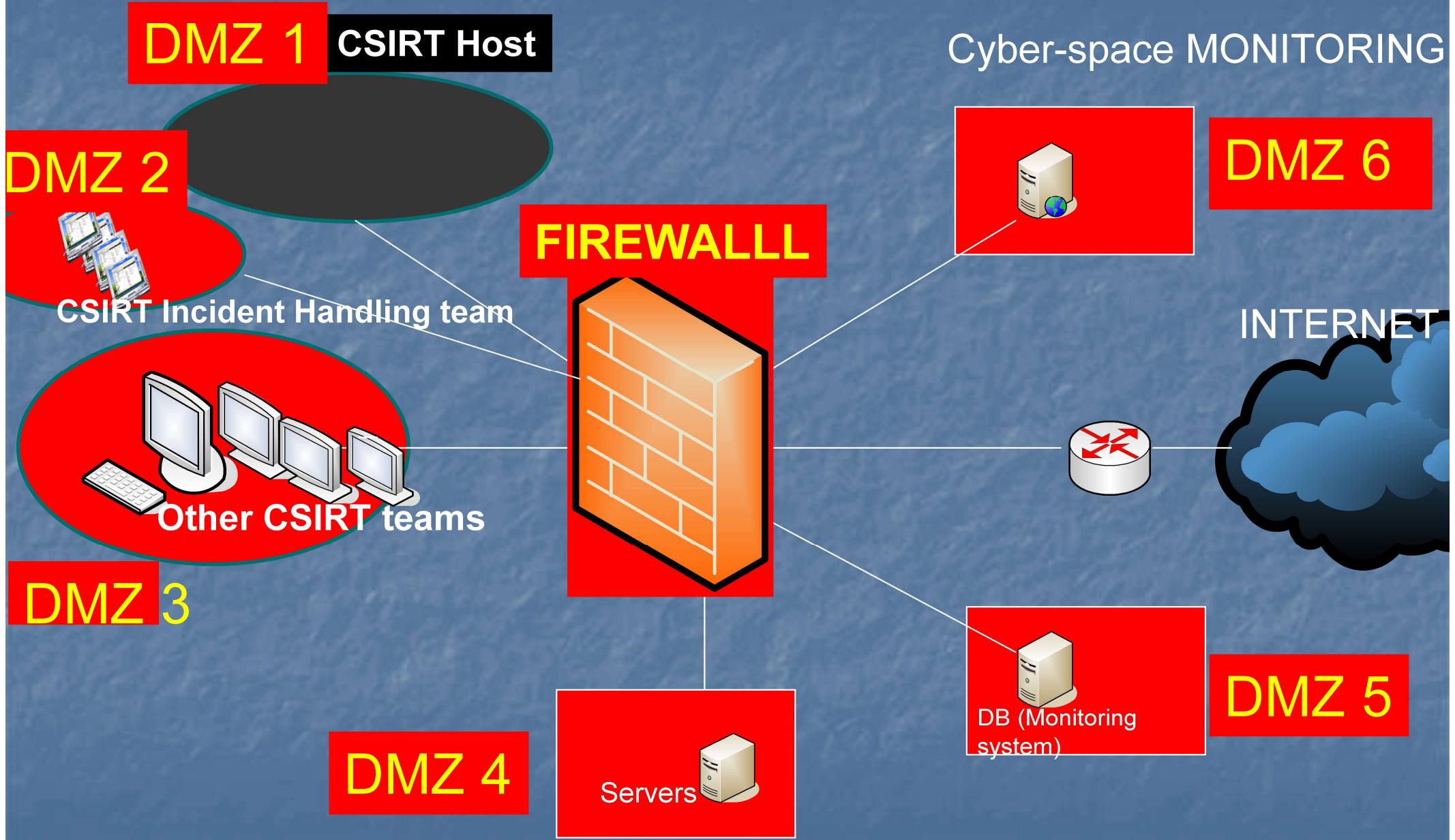
DO

- Filtering of IN (**and OUT**) Flows of communications
- Hiding of Network resources from “external bad eyes”.
- & Protection against Attacks based on vulnerabilities of communication protocols (packet fragmentation, DDOS, Spoofing of addresses, Syn flood,)
- + Permits to Divide the Protected Network into different zones of security (**DMZ**) with access control between these zones (sub-networks)

DOES NOT

- Does not Control **INTERNAL Attacks**
- Does not, by its own, Protect against **content threats** (Communication Content Control)

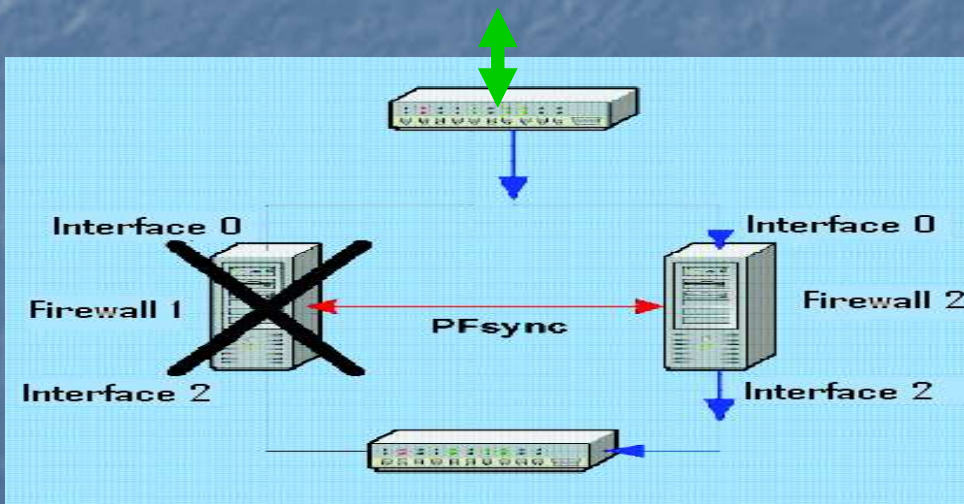
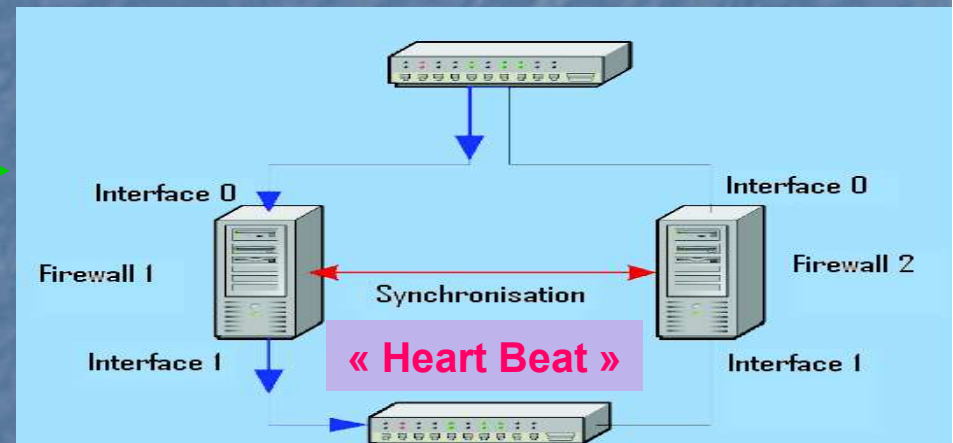
Segmentation in DMZs, via FIREWALL(s)



High Availability (HA) ?

A « Must », to avoid Risk of Network isolation

Normal scheme = All traffic go through firewall 1

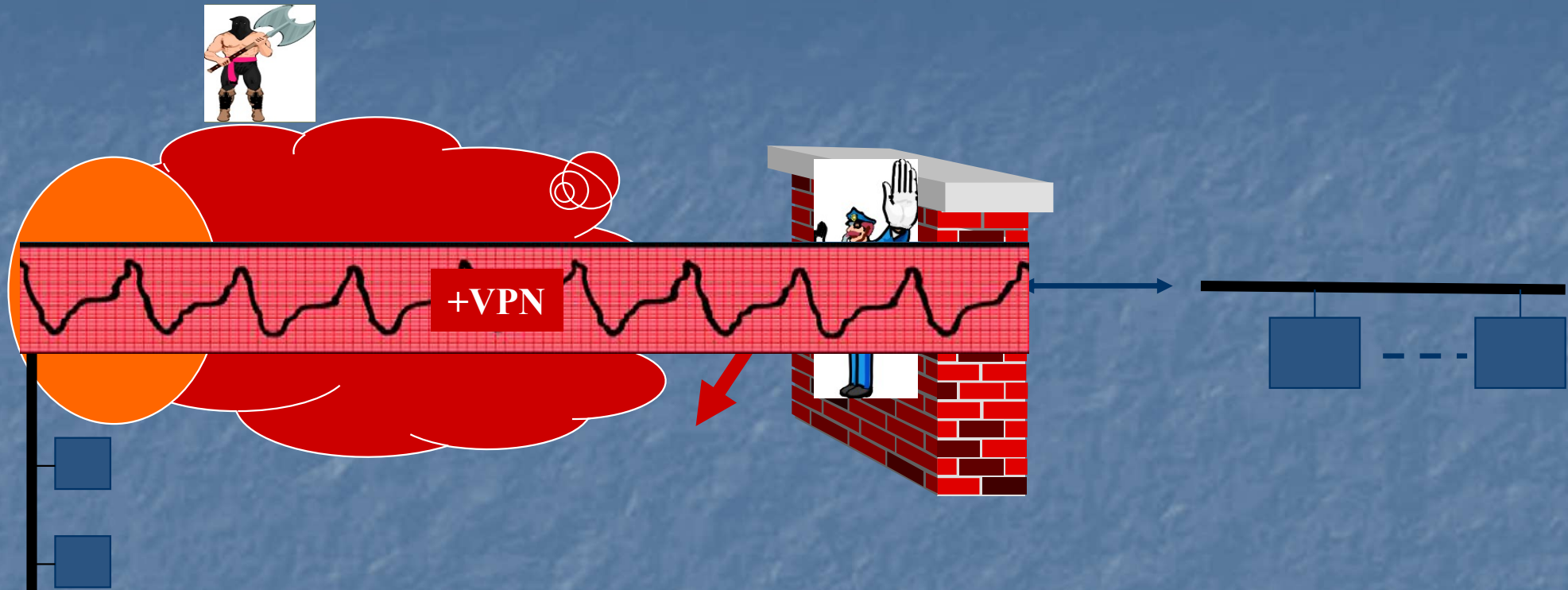


In case of firewall 1 Failure:

- Switch on firewall 2
- No connection break, thanks to synchronization between the two firewalls

→ OPEN-SOURCE offer HA: YES, via open source tools (CARP, pfsync, ..) on 2 Servers

Additional Functions assigned to Firewalls



Firewalls = CHECK Point for any IN/OUT communication flows

External Flows are relayed By the Firewall TO appropriate control servers
(Anti-Virus inspection, Intrusion detection, authentication....)

Are usually **Integrated** to the Firewall :

- **Content Inspection (Virus, intrusive flows)**
 - **UTM (Unified Threat Management) Firewall**
 - **NGFW (Next Generation Firewall/**
 - **“Deep Inspection Fw “**

-->**ACCESS CONTROL : Authentication server**

Stateful Firewall with very rich Filtering capabilities &

- Numerous features allowing granular control of the flows & **Various options of filtering** (filtering by Operating System, Transparent layer 2 firewalling, Limitation of simultaneous connections ...)
- **web interface for the configuration** of all included components + Graphical Reporting and Real Time Monitoring (RRD and SVG graphs).
- Can be run in many **virtualization environments**
- **High Availability** (CARP, Pfsync) +/- **load balancing**
- **Multi-WAN functionality, with failover** and NAT, DHCP Server and Relay

Pfsense Optional Tools (Packages) :

can be installed with one click. :

1. **Snort - IDS/IPS.**
2. **Snort - High Performance Network IDS, IPS and Security Monitoring engine by OISF.**
3. **OpenVPN Client Export Utility** - Allows a pre-configured OpenVPN Windows Client or Mac OS X's Viscosity configuration bundle to be exported directly from pfSense.
4. **tinc** - tinc is a Virtual Private Network (**VPN**) daemon that uses tunnelling and encryption to create a secure private mesh network between hosts on the Internet.
5. **stunnel** - An SSL encryption wrapper between the client and local or remote servers.
6. **Arpwatch** : monitors Ethernet to IP address pairing and logs changes to syslog.
7. **Ipguard-dev** - Attempts to maintain IP:MAC pairs by force.

AND Much More.....

Easy Integration/interoperability of OPEN-SOURCE solutions

Pfsense 's RICH Reporting and Monitoring tools

RRD Graphs

Maintain **Logs** of :

- Firewall states
- Individual throughput for all interfaces/Total throughput
- Packets per second rates for all interfaces
- WAN interface gateway(s) ping response times
- Traffic shaper queues on systems with traffic shaping enabled
- CPU utilization

SVG graphs (Real Time Information)

Show **real time throughput for each interface.**

- Real time display of queue usage.
- Real time CPU, memory, swap and disk usage, and state table size.

Host Platforms :

•Recommended : CPU - 1 Ghz / RAM - 1 GB

Can be installed on old PCs (small networks) : CPU - 500 Mhz /
RAM - 512 MB

How to Configure

Each packet is compared to a set of rules
(**ACL : Access Control List**)

- (rule 1, action 1)
- (rule 2, action 2)
- (règle 3, action 3)

Règle	Action	IP source	IP dest	Protocol	Port source	Port dest
1	Accept	192.168.10.5	194.154.192.20	tcp	any	25
2	Accept	any	192.168.10.3	tcp	any	80
3	Accept	192.168.10.0/24	any	tcp	any	80
4	Deny	any	any	any	any	any

...

- (rule-n: **ANY**, action-n: **DENY**)

- Firewall compare compliance of packet attributes
(IP/TCP/UDP Headers) to ACL rules
in sequential order

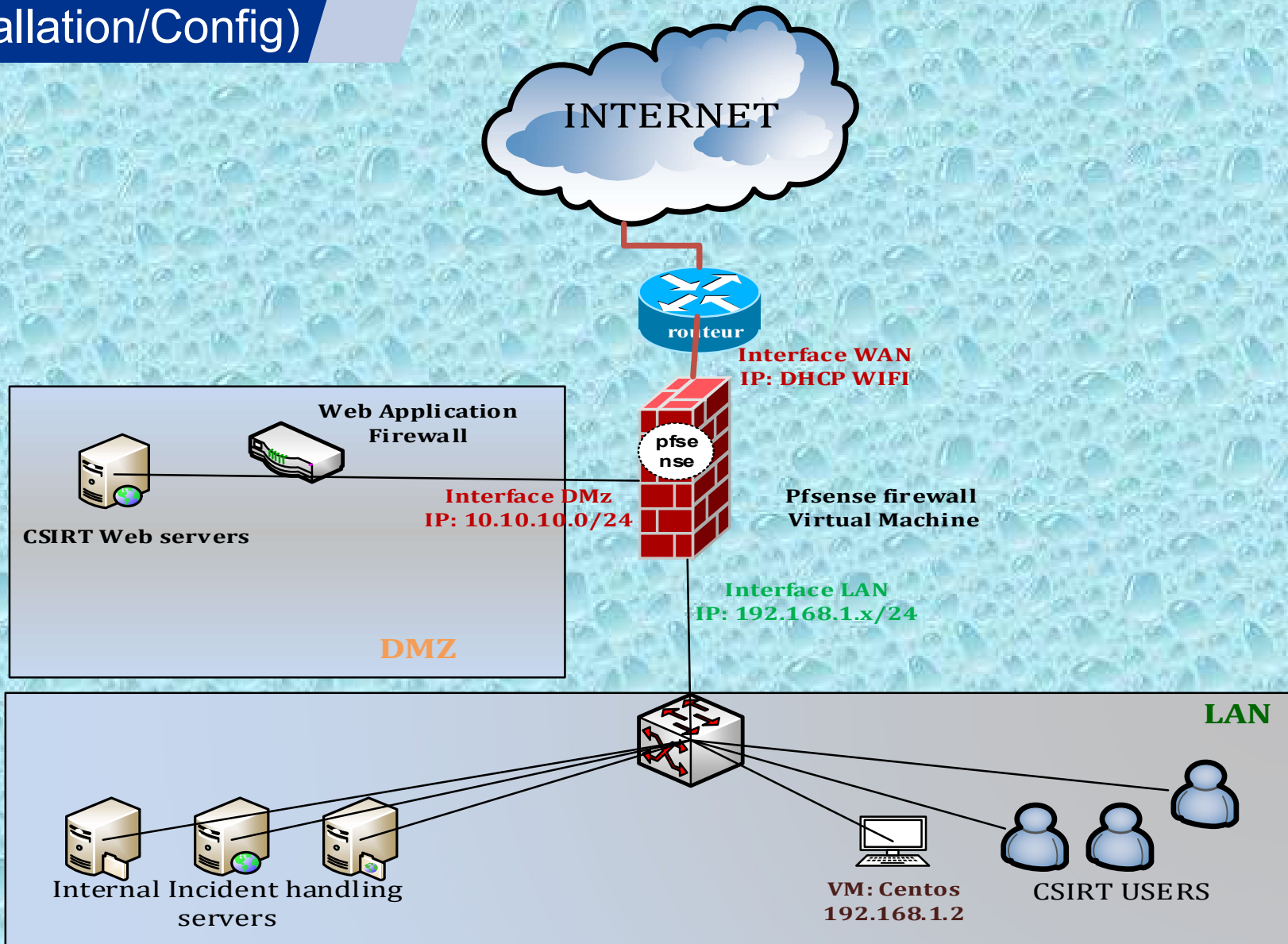
→ If A Rule is matched → Stop comparison and execute correspondent

Rich set of actions action : **Deny/Drop, Accept,**
/Relay the packet / Tag the packet

With easy configuration : http accept /

TRAINING PLATFORM : A VM (CSIRT NETWORK) WILL BE OFFERED (ONLINE) FOR YOU, AFTER THE TRAINING

+ Additional Training
(Installation/Config)





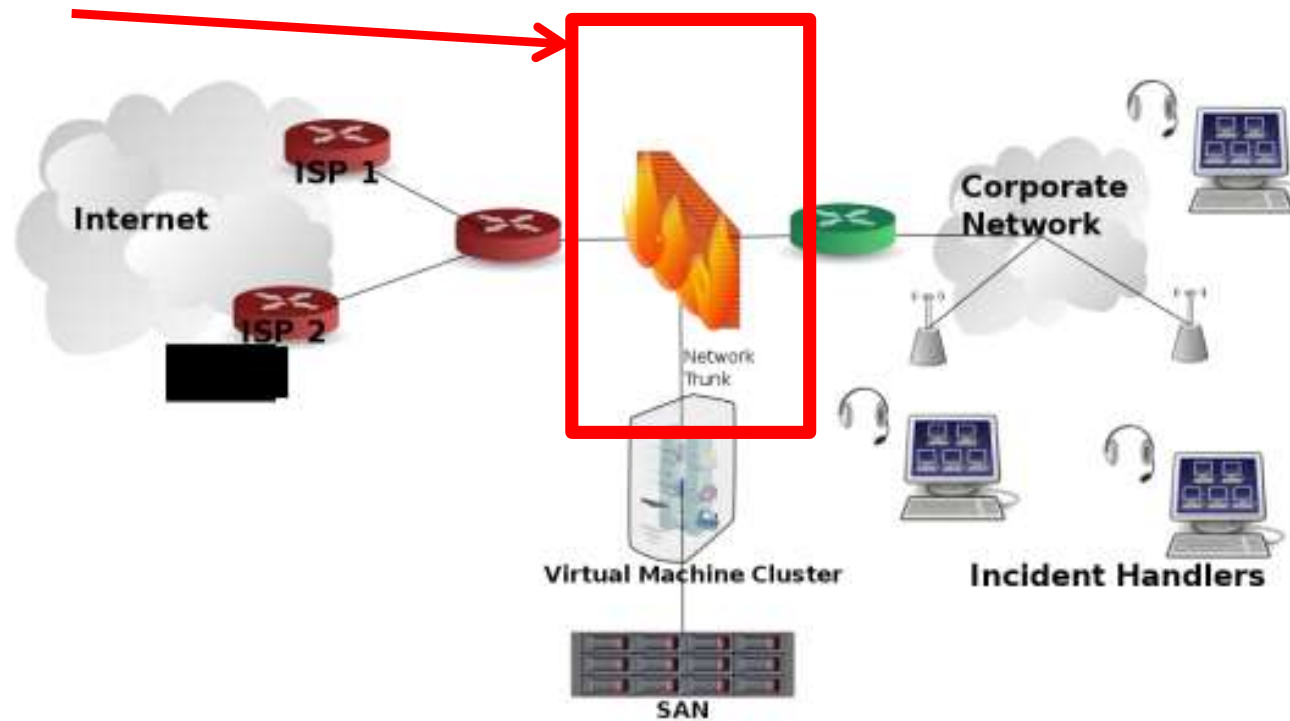
Pfsense



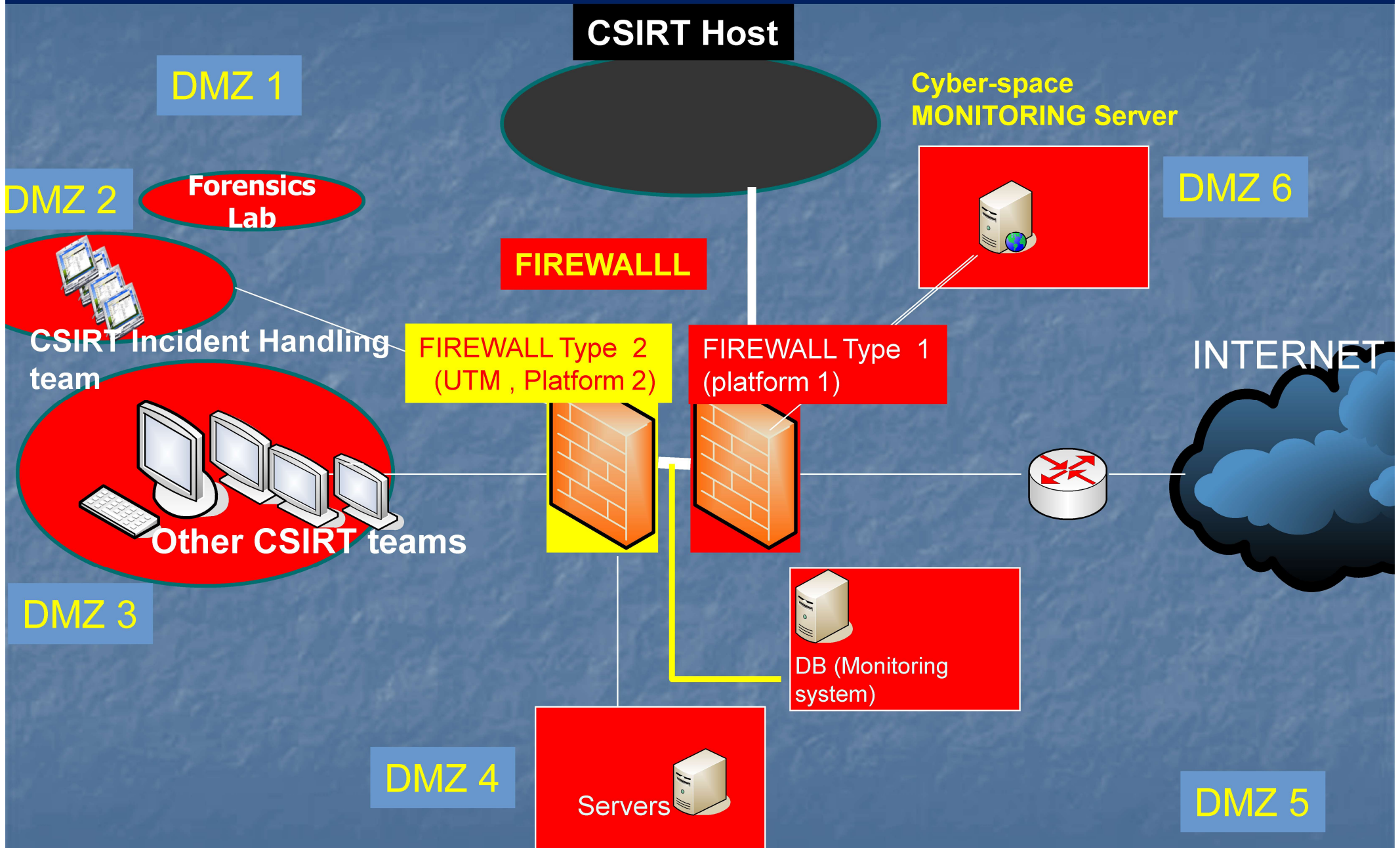
Eng Mondher
SMII, TunCERT

DEMO PLATFORM

Firewall : Pfsense



→ High Secure Architectures: Serial Firewalls (since Firewalls are based on, also, vulnerable software and platforms)



Multiple Open-Source Firewalls solutions available

Zorp GPL : Next generation firewall with deep protocol analysis: Network traffic analysis for layer 7 protocols/Encrypted SSL/TLS channel control/Content filtering (virus scanners, spam filters and URL checkers , ..) with optional modification (proxying)

<http://www.balabit.com/network-security/zorp-gpl>

NG Firewall Free, a basic UTM (Unified Threat Management) system, for medium size networks

ConfigServer Security Firewall, supports almost all Virtualization environments like Virtuozzo, OpenVZ, VMware, XEN, KVM and Virtualbox, <http://www.configserver.com/cp>

SmoothWall <http://www.smoothwall.org>

Endian Firewall Community, <http://www.endian.com/en/community/>

ShoreWall (NetFilter), <http://shorewall.net/index.html>

m0n0Wall, <http://m0n0.ch/wall/>

ISP-FW, <http://isp-fw.sourceforge.net/>

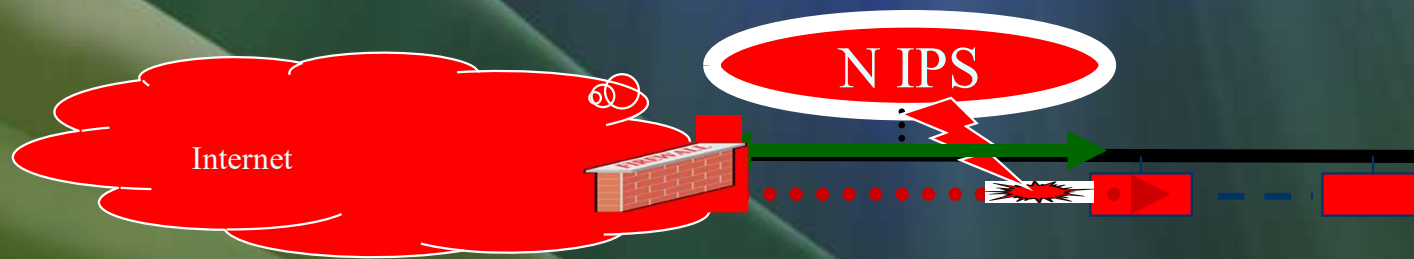
IPFire , <http://www.ipfire.org/>

ShellTr: <http://shellter.sourceforge.net/>

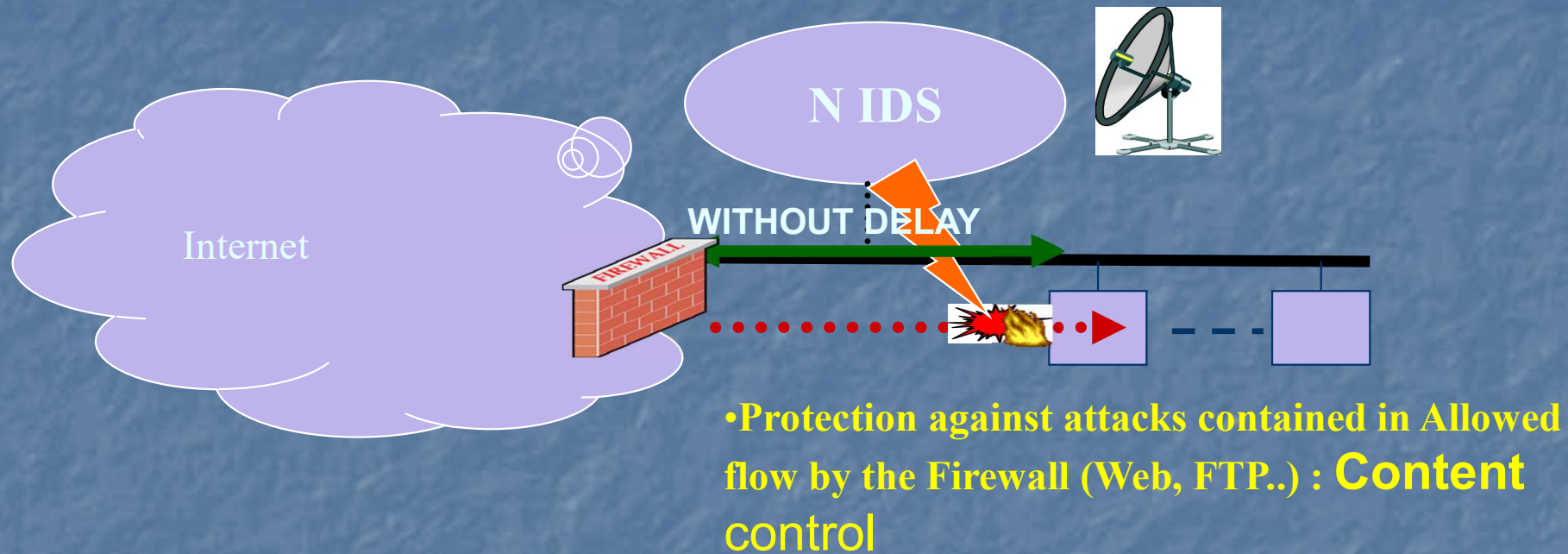
FirewallPAPI: <http://sourceforge.net/projects/firewallpapi/>

WIPFW: <http://wipfw.sourceforge.net>

Intrusion Detection : Network IPS and Host IDS



Network IPS : How it Works



Without delaying legitimate flows (sniffer), Detects attacks having passed the firewall (External flows) or originating from the **inside of the Network**, by observing a signature of an attack while packet are flowing through the LAN

→ Alerts and Logs

→ + Can **STOP Immediately** the attack (**IPS**) and/or modify the Firewall's **Rules**, to block an Intrusive External address, for **UDP intrusive flows**

Network Intrusion Detectors Systems (NIDS/NIPS)

Snort



- THE "OLDEST MUST"

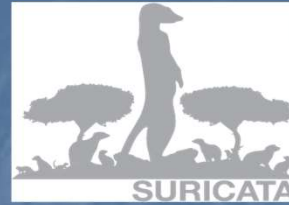
→ Pb : You should pay for « fresh » signatures (from 2011)
→ 399\$/year /sensor, for Business usage
(29,99 \$/year, for educational/personal use purposes)

but

→ **Still Open-source** (also after acquisition by **Cisco** in 2013)
& Signatures of attacks of **(Month-1 !!) still free,**

More NIPS

Suricata



Suricata combine **intrusion prevention (NIPS)** + network security monitoring (NSM) and PCAP processing,
Developed by the **OISF**.

A **high performance** Network IPS and Network Security Monitoring engine.

--> Multi threaded engine that take full advantages of multi-core processors

→Able to achieve Efficient Intrusion detection on **High speed traffic** without sacrificing rule set coverage.

<https://suricata.io/>

Another NIPS



Bro

NIPS Based on the behavioural approach (violations of security policies) → **Detection of Zero-Day attacks**

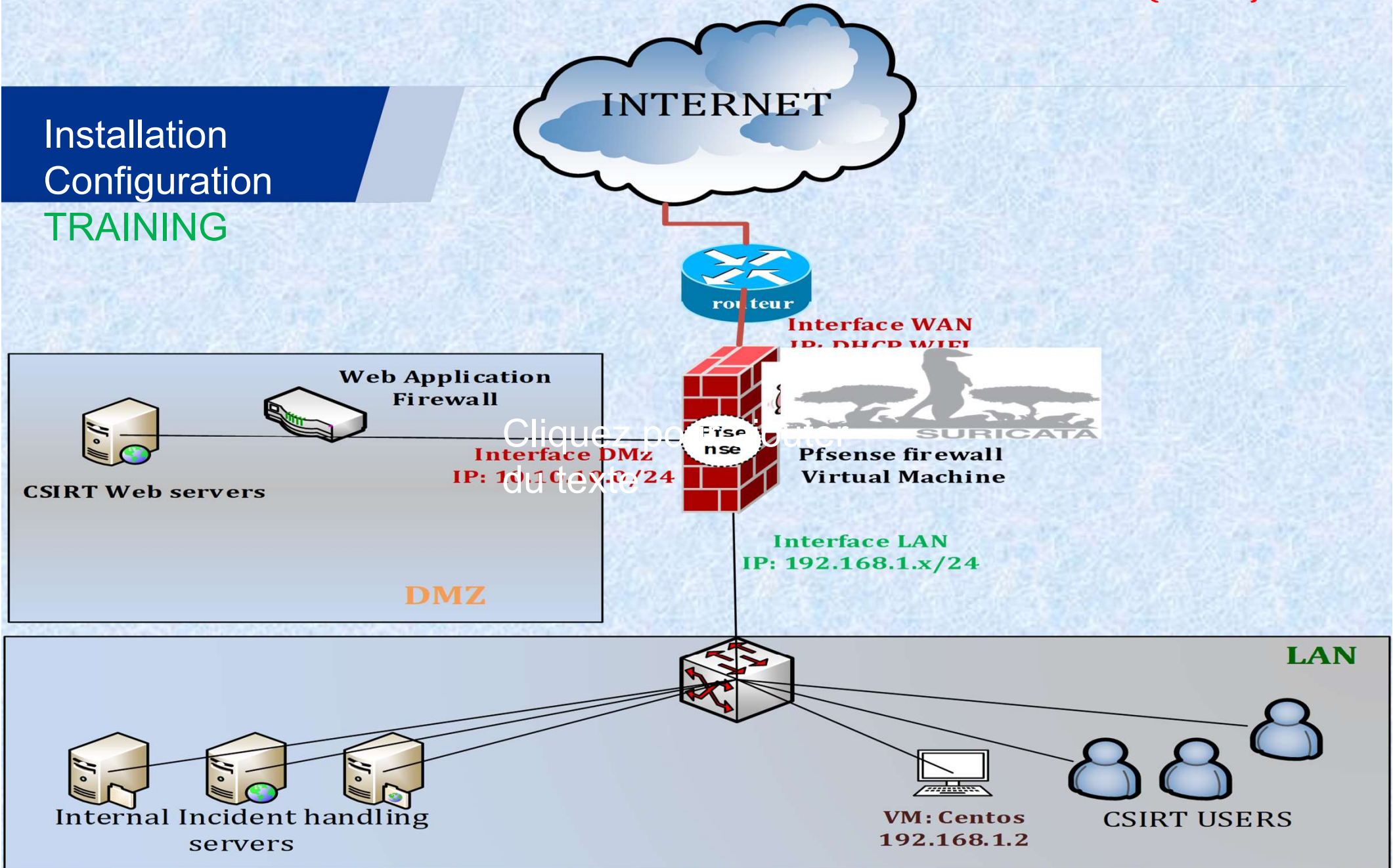
Developped by **Berkeley**

- Very powerful script Langage, for detecting new attack signatures
- Intrusion detection can trigger actions (NIPS)
- Compatible with Snort rules (converter snort2bro)
- Learning Mode (false positive)

<http://bro-ids.org/>

"AFTER TRAINING VM PLATFORM" : PFSENSE + IPS SURRICATA (IN LINE)

Installation
Configuration
TRAINING

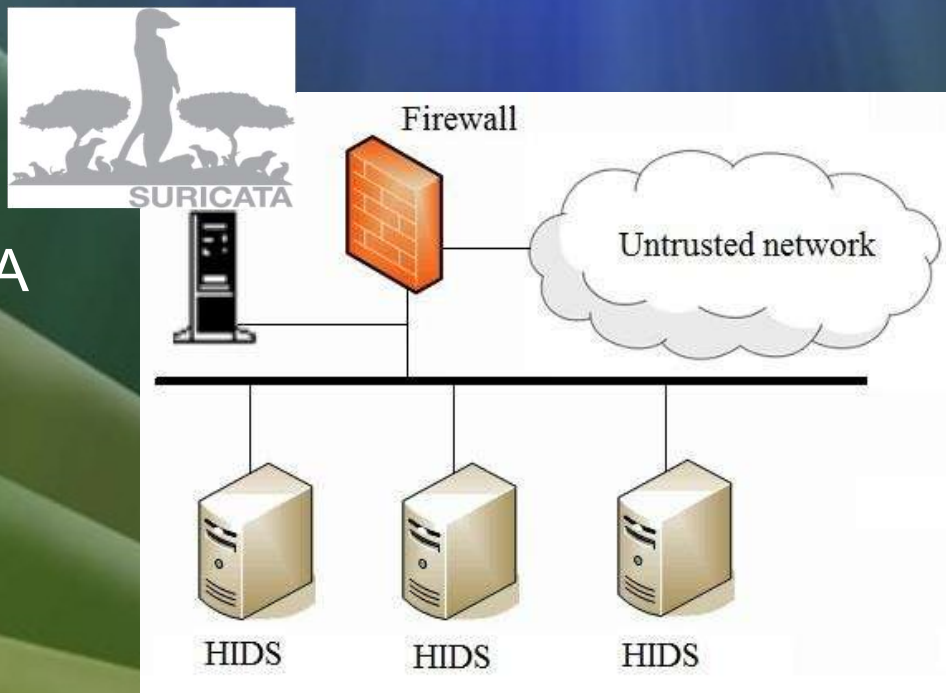




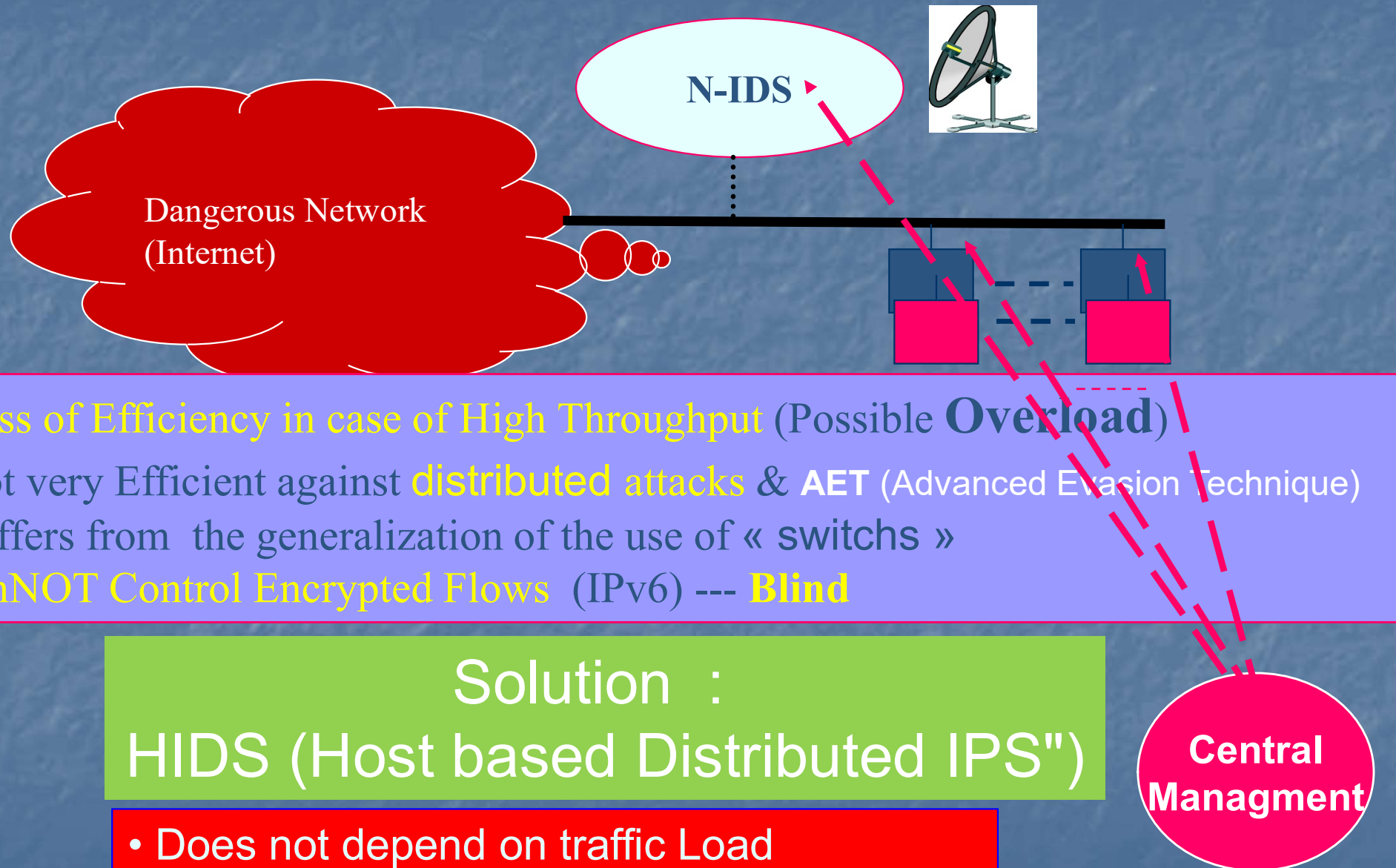
NIPS "SURRICATA"



SURICATA



Host IDS : HIDS



- Loss of Efficiency in case of High Throughput (Possible **Overload**)
- Not very Efficient against **distributed attacks** & **AET** (Advanced Evasion Technique)
- Suffers from the generalization of the use of « switches »
- **CanNOT Control Encrypted Flows** (IPv6) --- **Blind**

Solution :
HIDS (Host based Distributed IPS")

- Does not depend on traffic Load
- Efficient against distributed attacks
- **Permits VPN (IPv6) from Host-To-Host .**

Host Intrusion Detectors (HIDS)



OSSEC

Detection of rootkits, Log Analysis , File integrity check and process monitoring

- Available for Linux, MacOS, Solaris, HP-UX, AIX , Vmware ESX, and Windows platforms
- Can interact with an IPS
- Configurable Alert (via e-mail and handheld devices), and response (**HIPS**),
- provides a simplified **centralized management server** to manage policies across multiple operating systems
- **meet compliance requirements, as outlined in PCI DSS**

Samhain

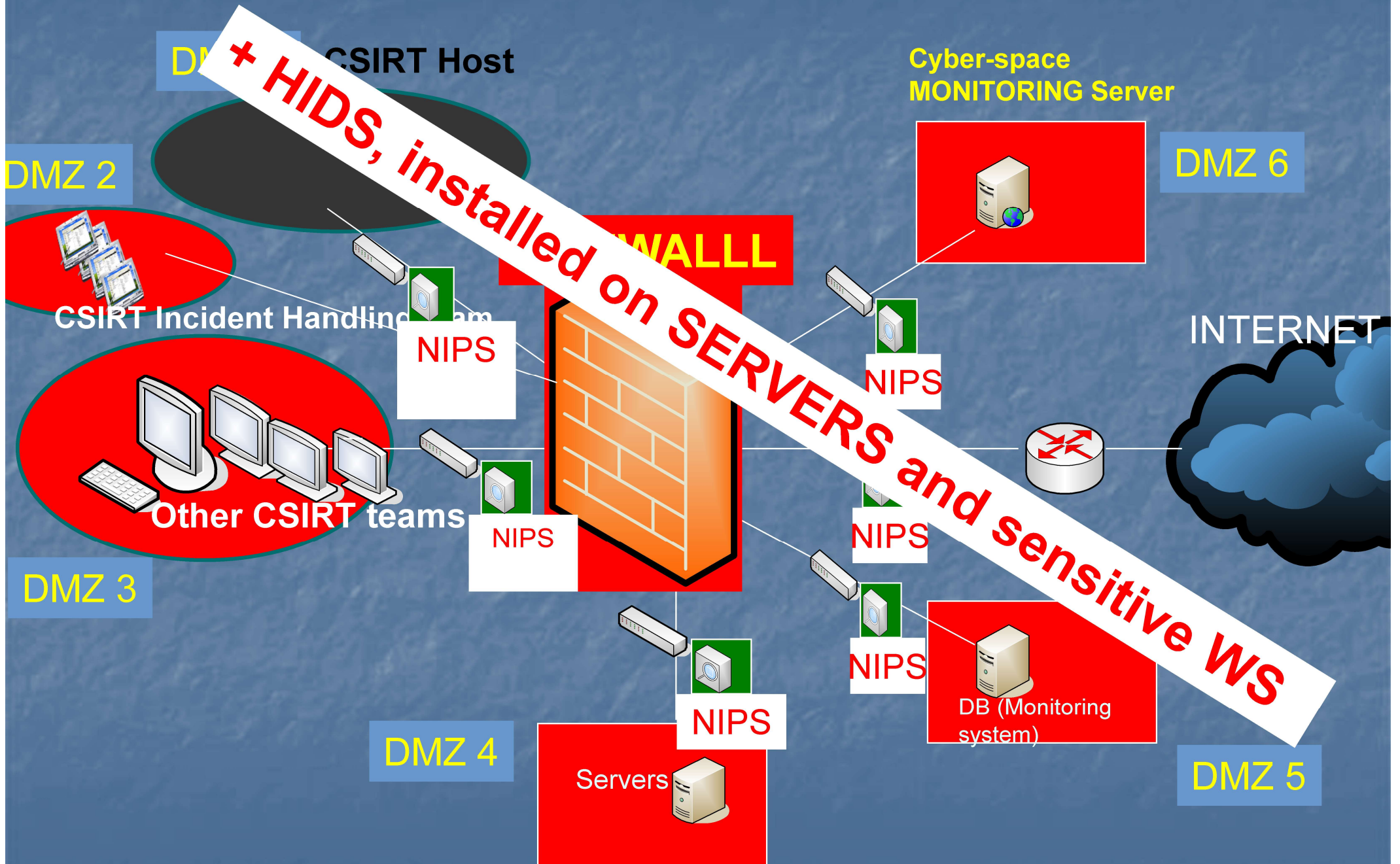


SAMHAIN LABS

Provides file integrity checking and log file monitoring/analysis, as well as rootkit detection, port monitoring, detection of rogue SUID executables, and hidden processes.

+ **centralized logging and maintenance.**

Deployment of Network IDS : Multiple (free licenses) NIPS (NIPS on line) + HIDS





Administration Tools :
Various Powerful tools for Log
processing and Alerting

SIM(Security Information Manager)/SEM (Event) /SLM (Log)



Prelude OSS Open Source version of Prelude implements a Security event manager (**SEM**)

BASE Provides a web front-end Sec Log Manager, based on ACID, to query and analyze the alerts coming from a SNORT NIDS system(**SIM**).

Sagan

Real-time log analysis & **correlation engine**

Supports event-driven script execution, GeoIP detection/alerting,

Supports many output formats

→ Maintain compatibility with Snort-oriented rule management software (*oinkmaster* ...) and consoles (Snorby, Sguil, BASE, and Prelude).

Swatch : **Alerts** when it matches the configured **log file entries** with your directives (regular expressions), **SEM**

syslog-ng : allows to flexibly **collect, parse, classify, and correlate logs from various platforms**, store or route them to log analysis tools (**SLM**).

SIEM : **Security Information and Event Management**

OSSIM

A **SIEM**, with event **collection, normalization and correlation**

-> give a view of all the security-related aspects, by **combining Log data + Asset data + Discovery data**

from various **information security controls and detection tools**

→ **Correlation** to create contexts to the information **not visible from one piece alone.**

OSSIM features a lot of Open-source **components**:

- Snort, or Suricata , as NIPS,
- Ossec as HIDS
- Nagios for traffic analysis

And much more :, Tcptrack, Munin, PRADS , NFSen/NFDump, FProbe, ...

+ self developed tools (a generic correlation engine with logical directive support and logs integration with plugins).



Open-source vulnerability Scanners

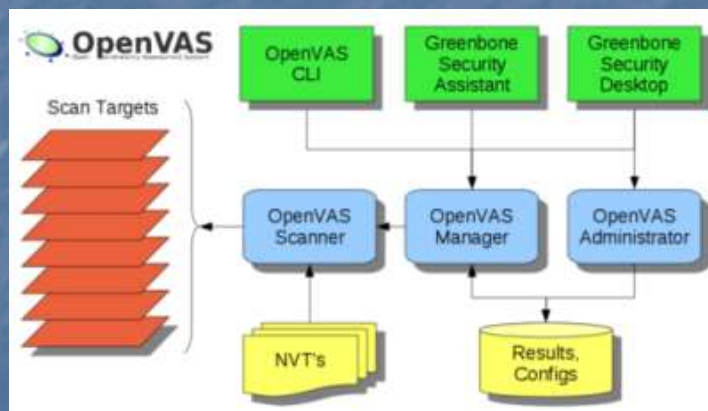
Open-source vulnerability Scanners

OpenVAS



- Powerful **vulnerability scanner** and vulnerability management solution (Fork from **NESSUS**, which become commercial in 2008).
- Daily update of Network Vulnerability Tests (NVTs),

A service-oriented client-server architecture: several modules, which communicate via well established protocols, SSL-secured.



<https://www.openvas.org/>

Open-source Web scanners



NikTo :

Web server scanner for multiple items, including :

- over 6700 potentially dangerous files/programs
- checks for outdated versions of over 1250 services
- checks for Version specific problems on over 270 servers.

skipfish by GOOGLE,

Carry out a recursive crawl of web sites, with **dictionary-based probes**.

→ Produce a map of the web site, annotated with the output from security checks.

whisker



Webscarab



/Websecurify



/Paros



Burp Suite, Netsparker,
w3af, Arachni,

Kali Linux : Linux distribution (Live DVD), regrouping all open-source tools for **Vulnerability Assessment and PenTesting**.
→ **allow complex vulnerability assessment scripts** :

More than 600 Tools :

- INFORMATION GATHERING
- VULNERABILITY ANALYSIS

Pen Testing :

- WIRELESS ATTACKS
- WEB ATTACKS
- EXPLOITATION TOOLS
- STRESS TESTING
- SNIFFING & SPOOFING
- PASSWORD ATTACKS
- MAINTAINING ACCESS
- REVERSE ENGINEERING
- HARDWARE HACKING
- REPORTING TOOLS

+ **FORENSICS TOOLS**



User Access Control

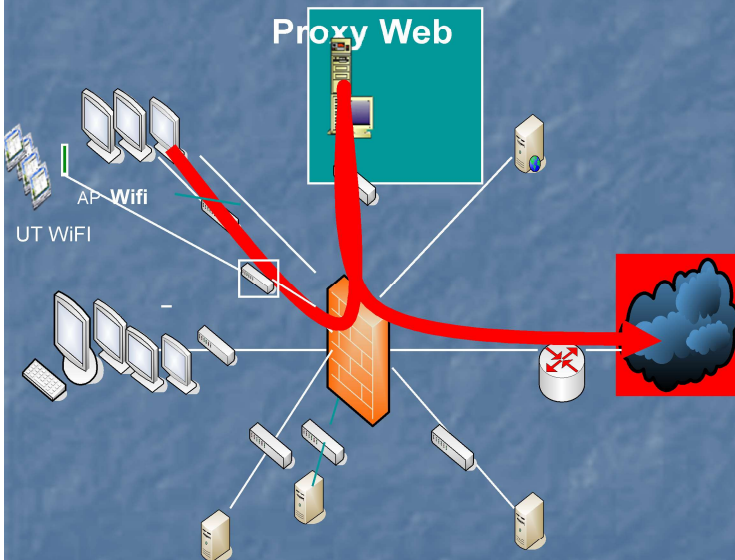


Squid Guard



✓ Extension of the « proxy » SQUID
→ URL Filtering

- By keyWords (**sex, ...**), with **regular expressions** support
- By Lists :
 - Access allowed to ONLY list of urls (Whitelists)
 - Access prohibited to ONLY list of urls (Blacklist)
- classes of Urls (news, sport, adultes, etc...).
- ...



--> Easy Configuration of the Firewall Rules

Single Sign On (**SSO**) solutions

Shibboleth (*Internet2*) SSO tool.



That Implements the OASIS SAML Language, to provide a federated single sign-on and attribute exchange framework.

+ **Offers 2 APIs** : OpenSAML-C++/Java

CAS (Yale University)



→ Provides **SSO (Single Sign On) protocol** for 3-Tiers applications

→ Offers CAS-clients for various plateformes (Java, .Net, PHP, Apache, ...)

Antivirus /Anti Spam

Antivirus Proxy

ClamAv

- One of the **Best Anti-virus Engines**
 - Anti-virus proxy for mail server
- Acquired by **CISCO** in 2013, but **STILL Open-source**,



RazorBack



Framework that allow in-line blocking on “store and forward” services, such as email services or web proxies,

→ coordinate the response against **Advanced Persistent Threats (APT)**, by permitting to implement **customized enterprise- and threat-specific detection and remediation.**

Workstation solutions

Freeware **Immunet** ,

Based on the **Open source ClamAV engine**
Includes a Real Time Monitor

→ provides cloud-based protection, with no need to download any virus signatures
Immunet is up to 35 times lighter than other anti-virus solutions
PB: has to be connected to the Internet

ClamWIN

, open source, for Windows
Microsoft Windows XP/2003/Vista.
No real time monitor
+ No Central Administration



ClamXav

Free software for Mac OS , including Real Time monitor → become commercial
June 2015 ...

PB : Signatures Less « rich » than those of commercial ones
(task-force Problem)
+ A lot of comercial versions, free of charge for Domestic use

Open-source **Anti-Spam Gateways**

SpamAssassin

- Very popular (ISPs ...)
- Various techniques for Spam detection
(exclusion Lists, DNS, fuzzy-checksum-based, filtering Bayesian, blacklists, BD online).



ASSP Anti-Spam + Anti-virus Gateway

- integration of Anti-virus Plug-ins (ClamAV, ...)



+ Amavis



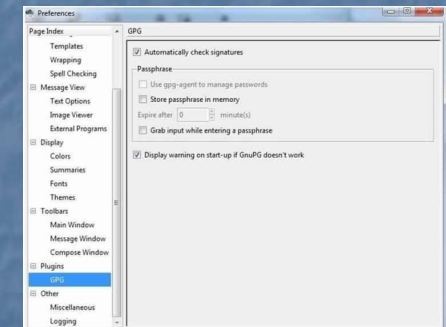
Tools for encryption of Communications and storage

GNU PRIVACY GUARD (GNUPG)

- Gnu Implémentation of the standard OpenPGP (RFC 4880, PGP).
- No algorithms under patent (Supports ElGamal, DSA, RSA, AES, 3DES, Blowfish, Twofish, CAST5, MD5, SHA-1, RIPE-MD-160 et TIGER).
- Includes a little PKI manager .



Windows Version of GPG



Disk encryption tools



VeraCRYPT

multi-platform Disk encryption software,

create a virtual encrypted disk within a file or encrypt a partition or the entire storage device with pre-boot authentication

→ based on **TrueCrypt 7.1a**, which development has been **abruptly** ended in 2004



DiskCryptor

offers encryption of any and all disk partitions, including the system partition

. Support various encryption algorithm (AES, Twofish, Serpent, ..., including their combinations).

- Transparent encryption of disk partitions.
- Full support for dynamic disks.
- Support for disk devices with large sector size (RAID).

VPN

SSL VPN

OpenVPN

- Offer various cryptographic algorithms (OpenSSL)
- Good Support of bulk connections (big number of simultaneous connections)
- Available for Linux, Windows, OpenBSD, FreeBSD, NetBSD, Mac OS



IPSec VPN



StrongSwan : Derived from FreeSWAN (2004), implements IPSec
For Linux, **Android** and **Mac OS X**



OpenSwan : Derived from FreeSWAN (2004), implements IPSec
For Linux and **Windows**,



VPN Client : IPsec client for Windows/Linux
→ VPN gateways for ipsec-tools, FreeSWAN, OpenSWAN, StrongSWAN, isakmpd)

+ of course :SSH

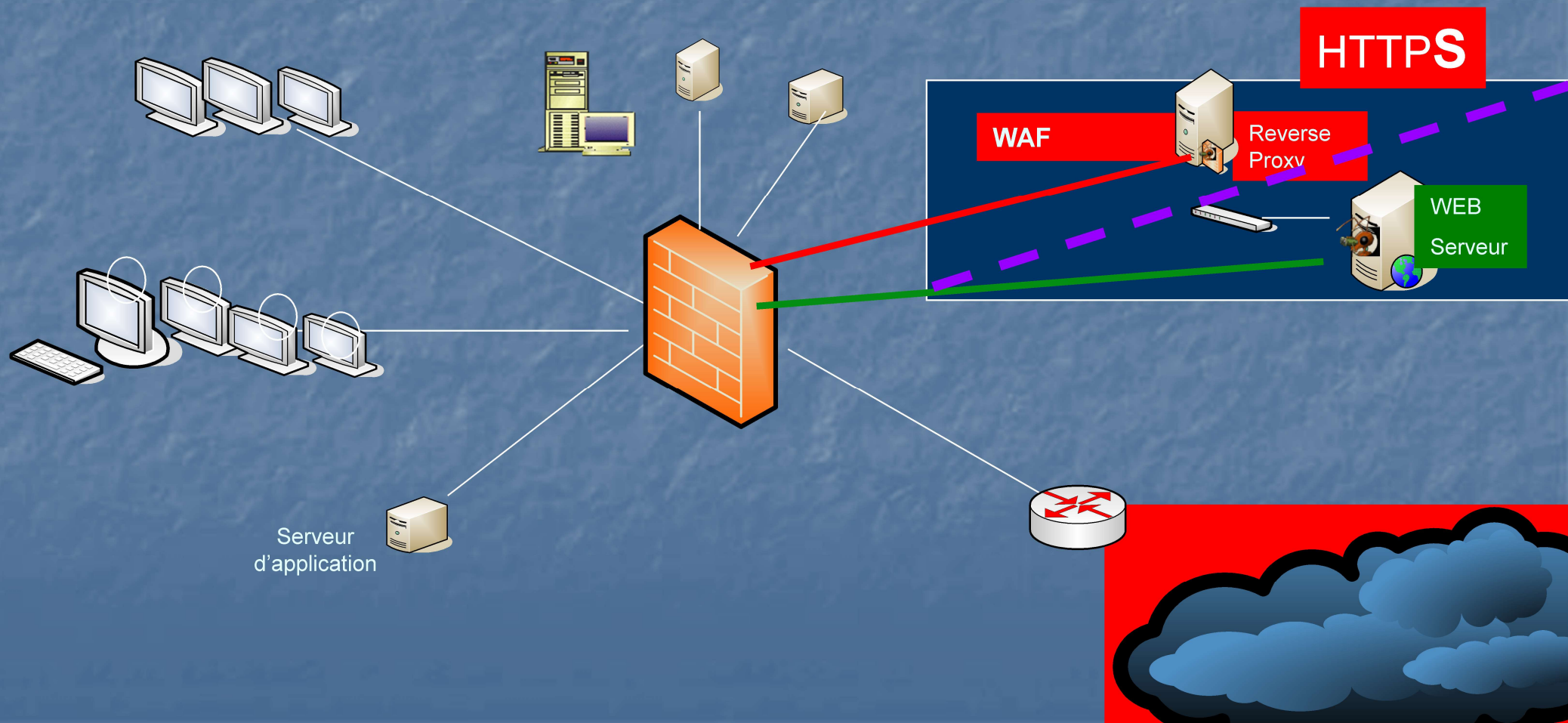




Protection of the CSIRT public Web server

Protection of the CSIRT Web Server

- Web Application Firewalls
- « Reverse proxy »
- HttpS



Open-source WAF

→ Inspect the HTTP traffic stream, in real-time, with event correlation. and reliable blocking.

ModSecurity

- Real-time Blacklist Lookups
- HTTP Denial of Service Protections
- Generic Web Attack Protection
- Error Detection and Hiding



+ **WAF-FLE** : an OpenSource ModSecurity Console

IronBee - WAF sensor intended for real-time monitoring



Open-source Toolkits, for HTTPS


mod_ssl

HTTPS for Apache servers (based on SSLey).

Apache-SSL

An Alternative, based on OpenSSL





Secure and Virtualization Platforms

Linux-VServer



- a **jail mechanism** in that it can be used to securely partition resources on a computer system
- > a **process cannot mount a DOS attack on anything outside their partition.**

Qubes OS



Implements a "*Security by Isolation*" approach :

- **Isolate the various environments**, so that if one of the components get compromised, the malicious software would get access to only the data inside that environment.
- not a multi-user system

SELinux (NSA & RedHat)

provides a mechanism for supporting access control security policies , including

DoD's **Mandatory Access Controls (MAC).**

AppArmor

→ includes a **learning mode**

Virtualization platforms

VirtualBox (oracle) : powerful Type 2 virtualization open source solution



Runs on Windows, Linux, Mac, ... : hosts and supports a large number of guest operating systems



Xen

open-source type-1 hypervisor (run directly on the host's hardware), and permit to run many instances of an operating system or indeed different operating systems in parallel on a single machine (or host).

Has famous users, that include cloud providers such as *Amazon Web Services*, *Rackspace Hosting*, *Verizon Cloud* and many others



And Much more

And Much more

FreeNAS ("TrueNAS")

Open source NAS system based on FreeBSD and the ZFS file system, with a dedicated management web interface.

- Supports RAID



JUST for ANNOTATING SPIRIT OF RESPONSABILITY In Open source
Openfiler freeware NAS/SAN

--> dev stopped in 2015 (after auto-criticism from authors, in 2013)



Video Control solutions

iSpy : open source



turns a PC into a full security and surveillance system

- Detect and record movement or sound.
- Captured media is compressed to flash video or mp4 and streamed securely over the web and local network.

Freeware ZoneMinder

Provide a complete surveillance solution for Large Corporation (capture, analysis, recording and monitoring of any CCTV or security cameras)





ROI ?

Able to deliver more CSIRT services :

- **Immediate Assistance** of the constituency in **rapidely deploying Security Architectures**, based on open-source security tools

(Leave Training + Assistance left to young private corporation --> Jobs)

- R&D: customisation/combination/enrichment of open-source tools



Overview about the implementation, with open source solutions, of a

- **National Cyber Space Monitoring System**
- **Honeynet System**
- **Artifact analysis Lab**



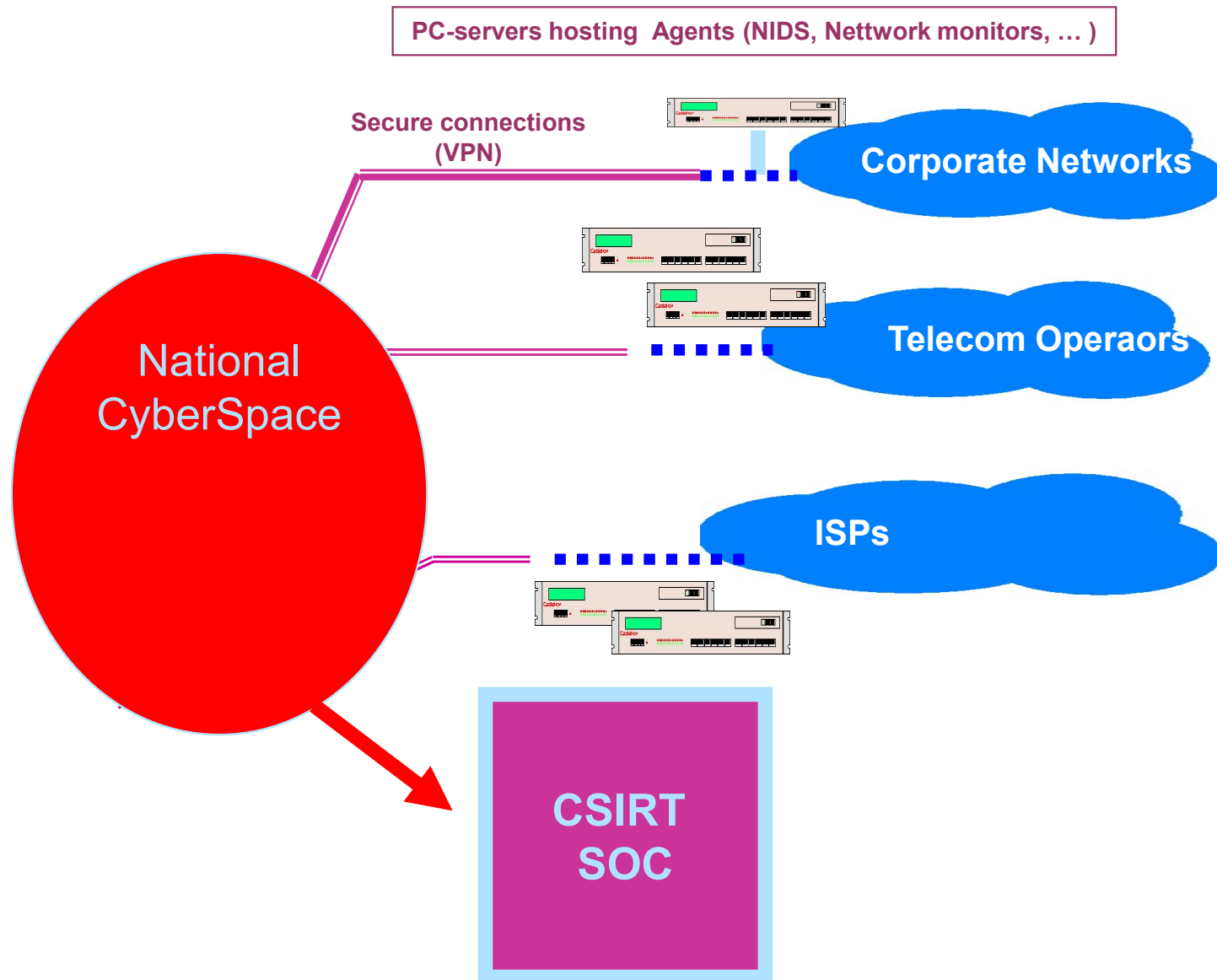
Cyberspace Monitoring System

Important to Not be BLIND about
« what is going on » in the National cyber-space

Cyber Space Monitoring System (CSMS)

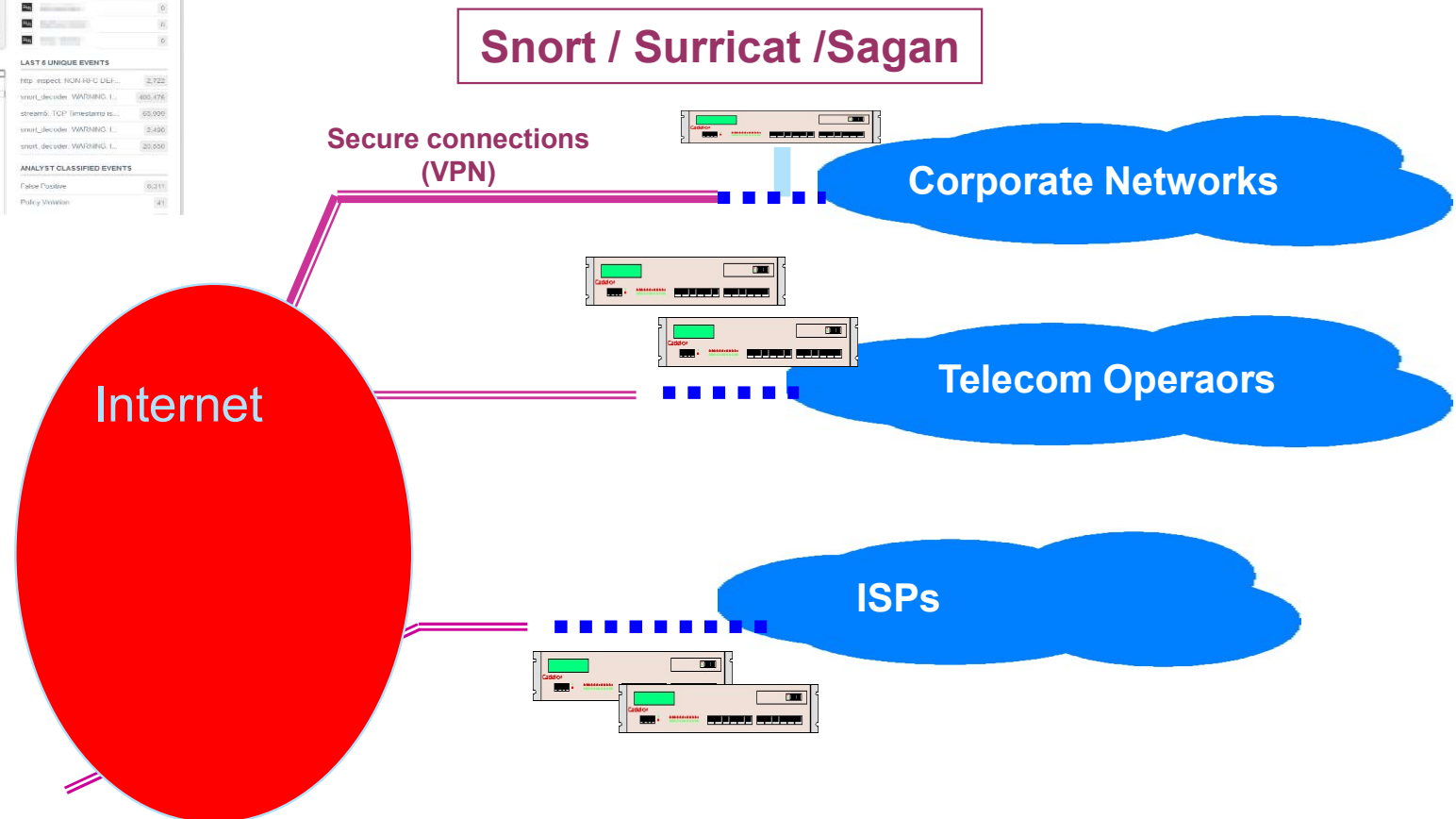
A **SOC** (based on **open-source solutions**), which permits to monitor the National Cyber-Space security in **Real time**

→ For the **early Detection** of **Massive attacks** and minimization of their impact.



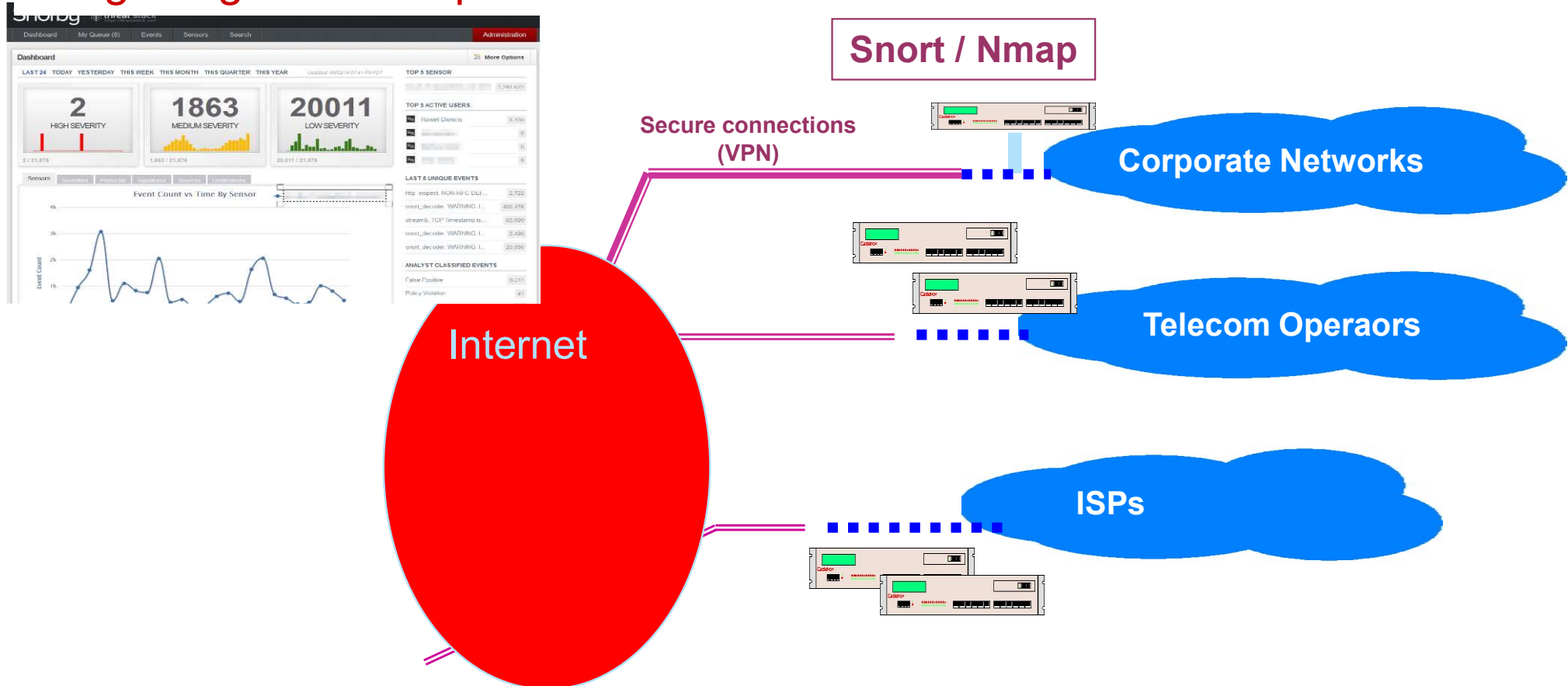
Simple Cyber Space Monitoring System (CSMS)

Snorby : a ruby on rails **SIMPLE** web application for network security monitoring that interfaces with current popular **intrusion detection systems** (Snort, Suricata and Sagan).



Richer Cyber Space Monitoring System (CSMS)

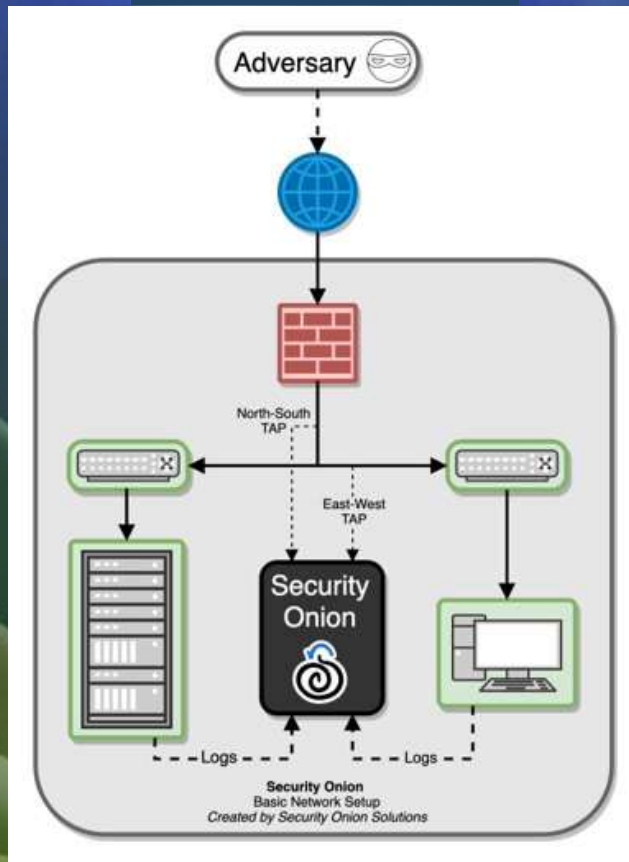
Security Onion : Simple and Rich Tool for CSMS,
integrating various open source **NIDS** and **NSM**



Integrate

:Suricata, TheHive, Playbook, Fleet, osquery, CyberChef, Elasticsearch, Logstash, Kibana, Zeek, Wazuh

Onion



« SAHER » :

**TunCERT System for
the Monitoring of
the security of the **Tunisian
Cyber Space****

- ❖ **A CSMS tool, with Correlation of incidents (logs) --> Automatic Alert**
- ❖ **Integrate Feeds from International Threat Intelligence Platforms and Honeynet systems**

Cooperation with other international CERT:
Recuperation of attacks from Tunisia

Incident Workflow:
Incident recovery

Open Source Vulnerability Database (OSVBD):
Source of information on vulnerabilities

SAHER-WEB

DotTN web sites monitoring
- Web Defacement
- DoS Web
- Deterioration of web access

SAHER-SRV

Internet services availability monitoring:
- Mail Bombing
- Breakdown of DNS servers
- DNS poisoning

SAHER-IDS

Massive attack detection:
- Intrusion
- DDoS
- Viral attack

SAHER-HONEYNET

Malware gathering:
- Viral attack
- Scan
- Possible attacks

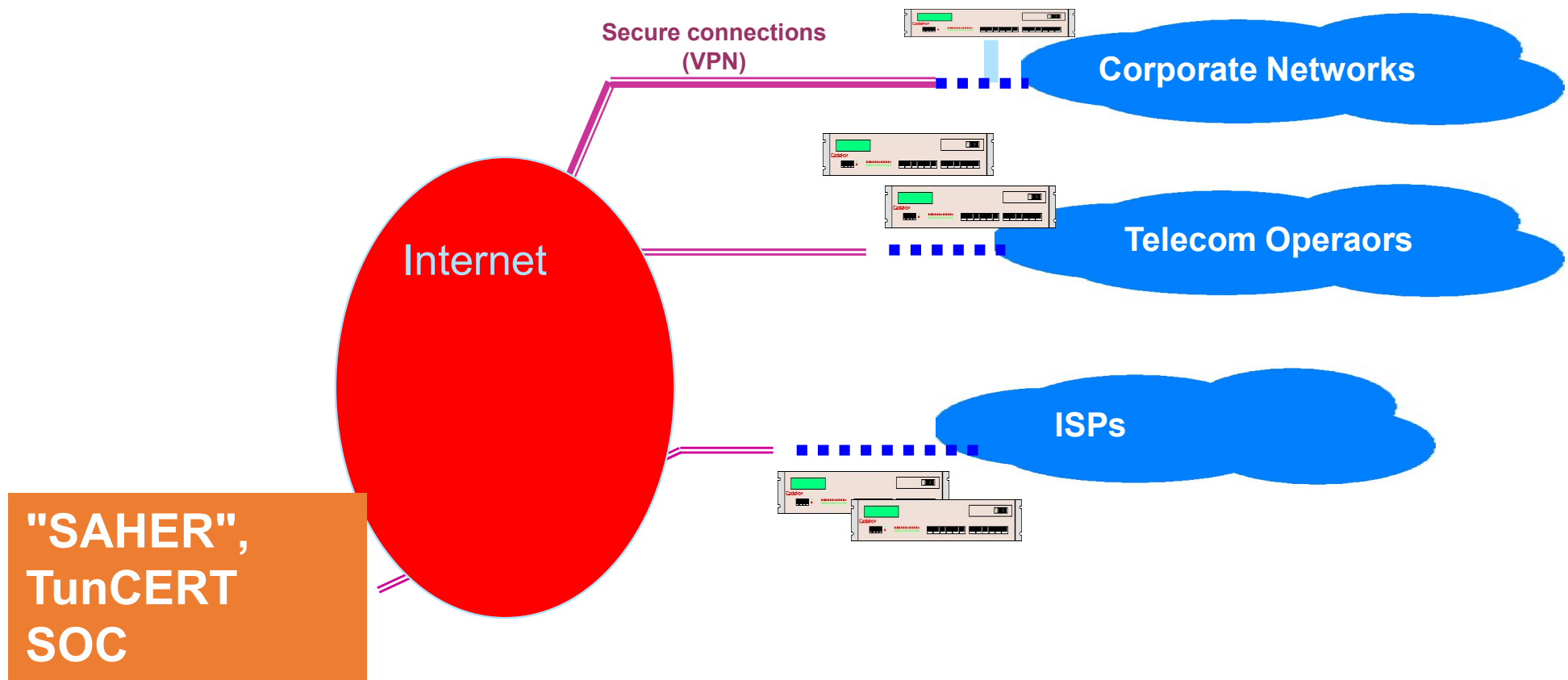
Correlation

Incident handling

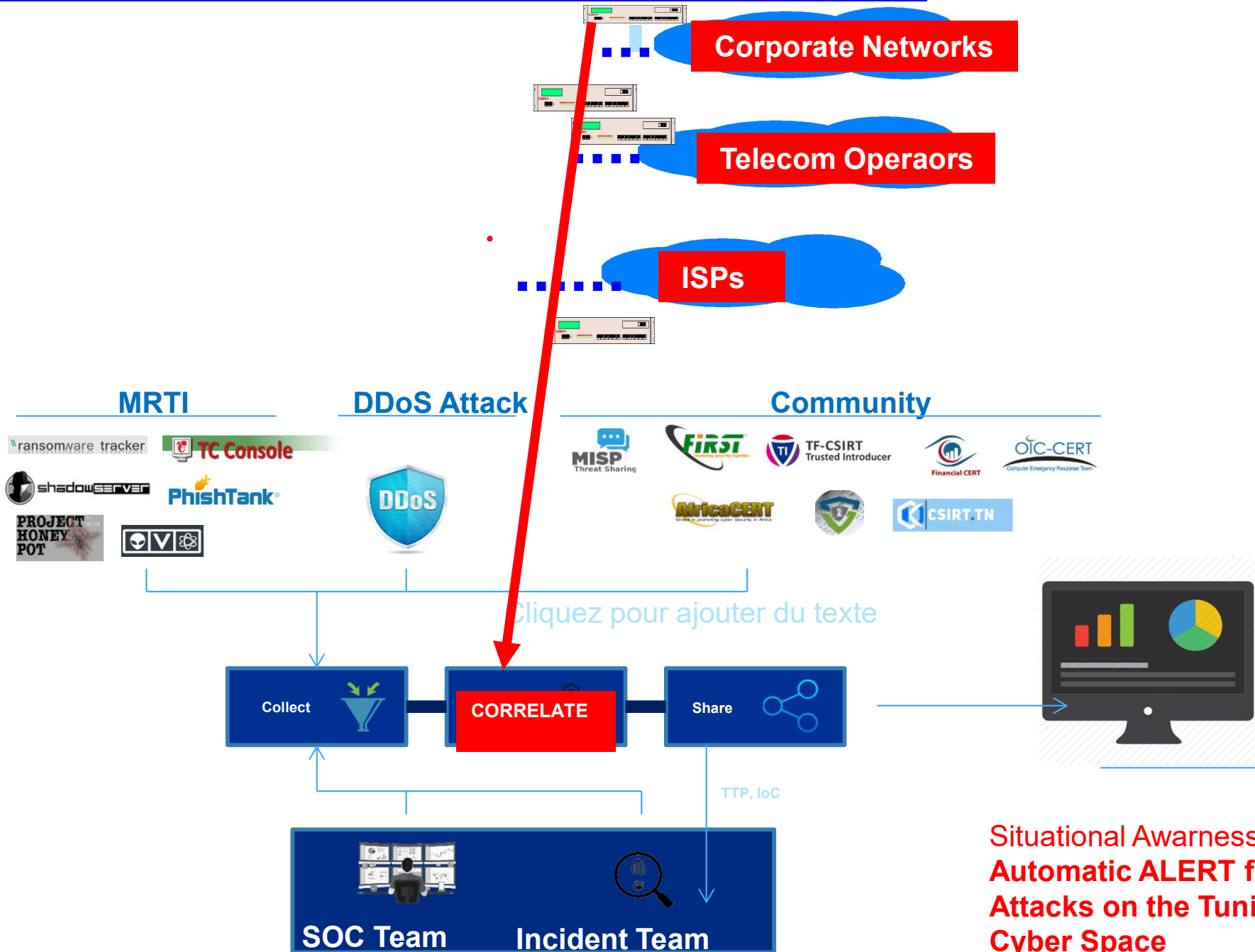
Watch

Detection and tracing of cyber attacks

System "SAHER"

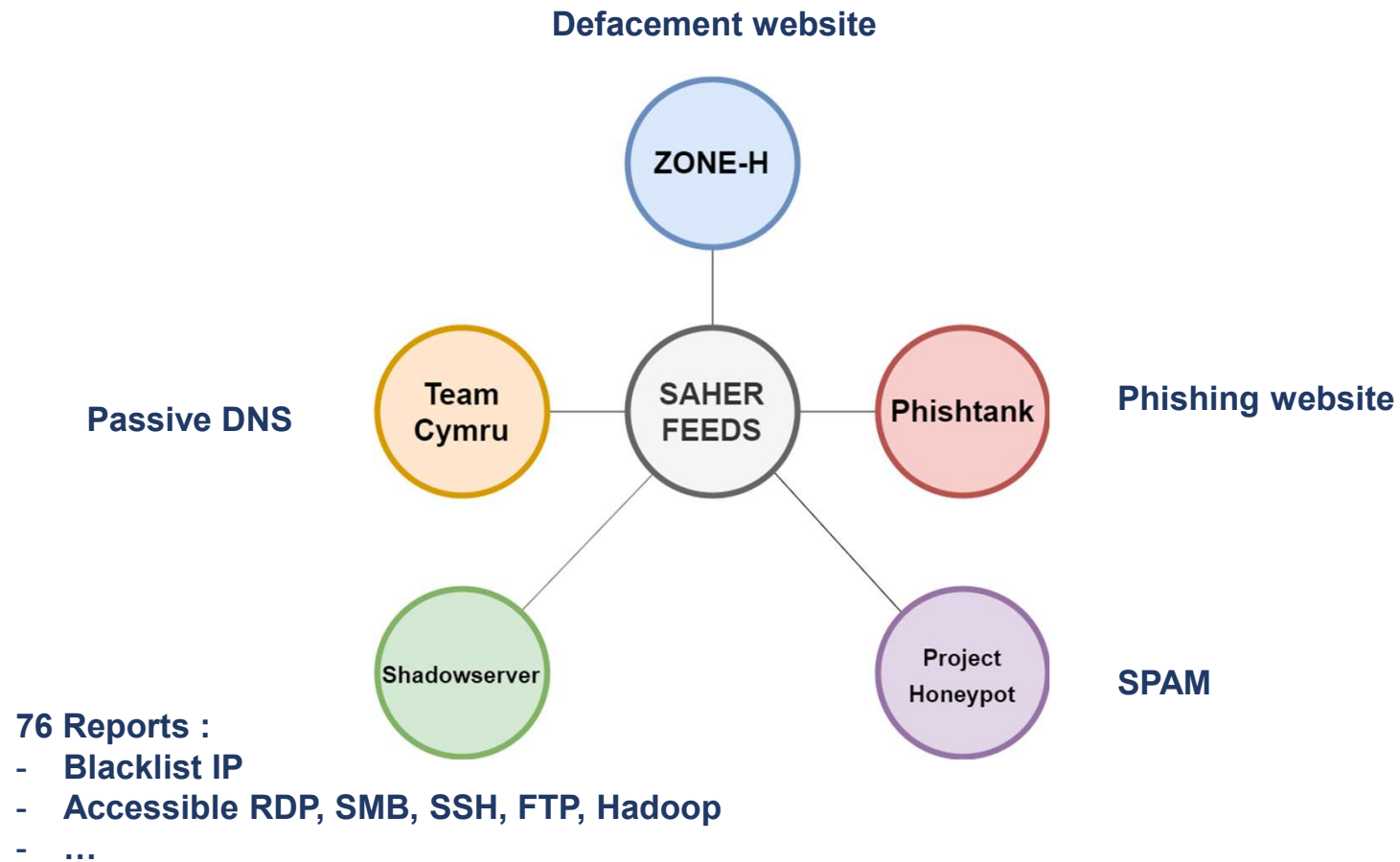


System "SAHER"



Situational Awareness :
Automatic ALERT for Mass Attacks on the Tunisian Cyber Space

THREAT FEEDS





FAST DEMO of "SAHER"

HoneyNet Infrastructure, For Artifact (malware, hacking toolkits/scripts discovery & capture)

+

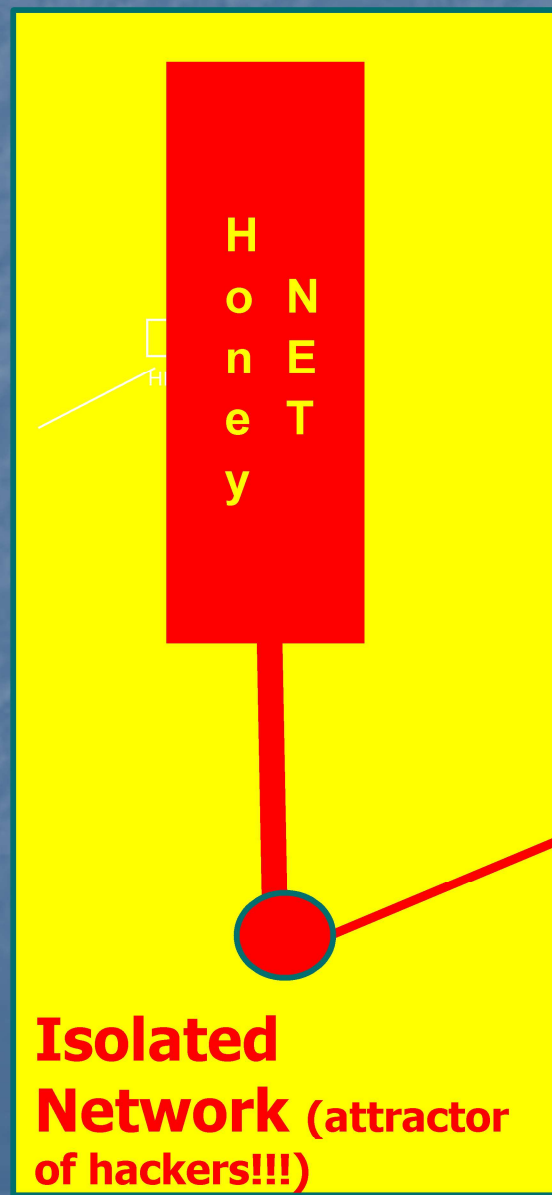
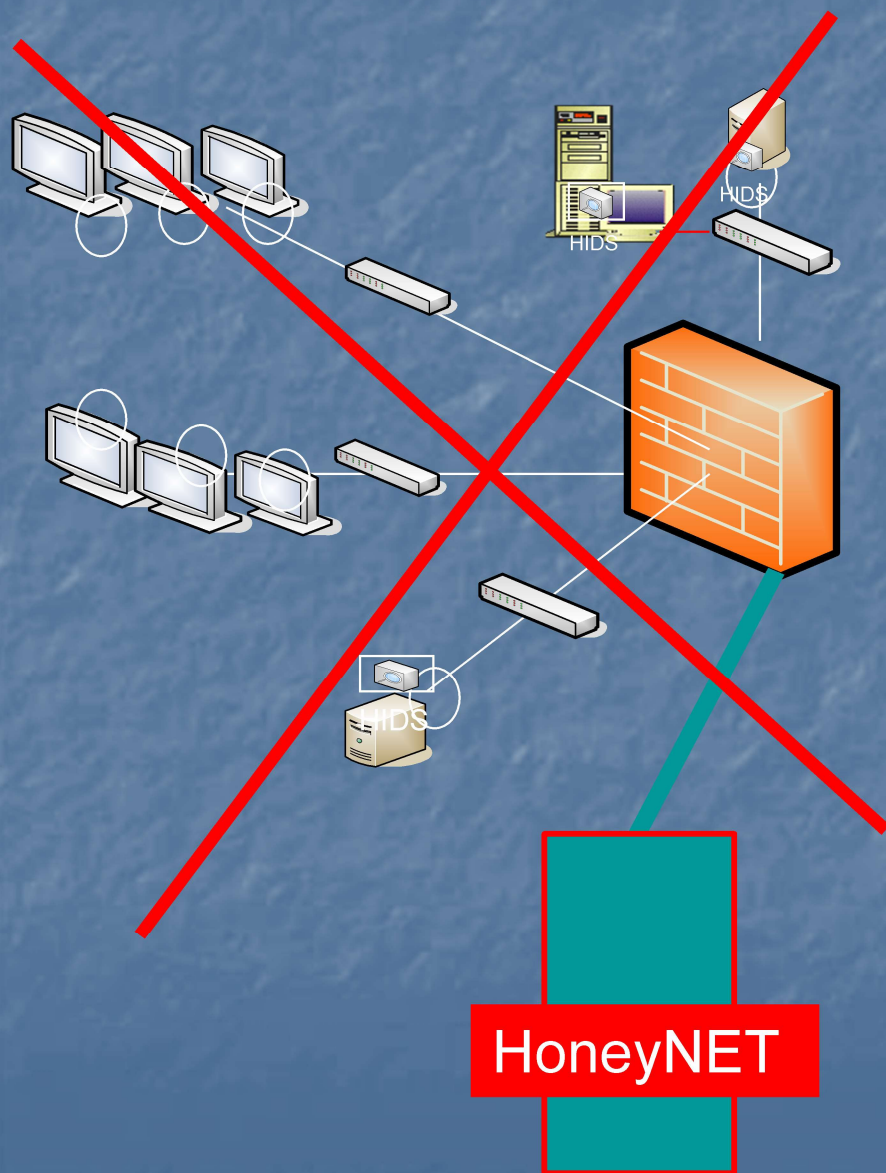
Permits also to let your constituency (mainly ISP) believe
In your supervision of the security of the cyber-space (bots,
worm propagation, ..)

Permits to capture **samples of** threats (bots,
worms payloads...)

IS NOT a CSMS

« Honey-Nets »

« Attract » and « jail »
intrusion toolkits/artifacts



emulate Virtual
vulnerable
machine/
Services
(/Networks)

« Dirty » IP address

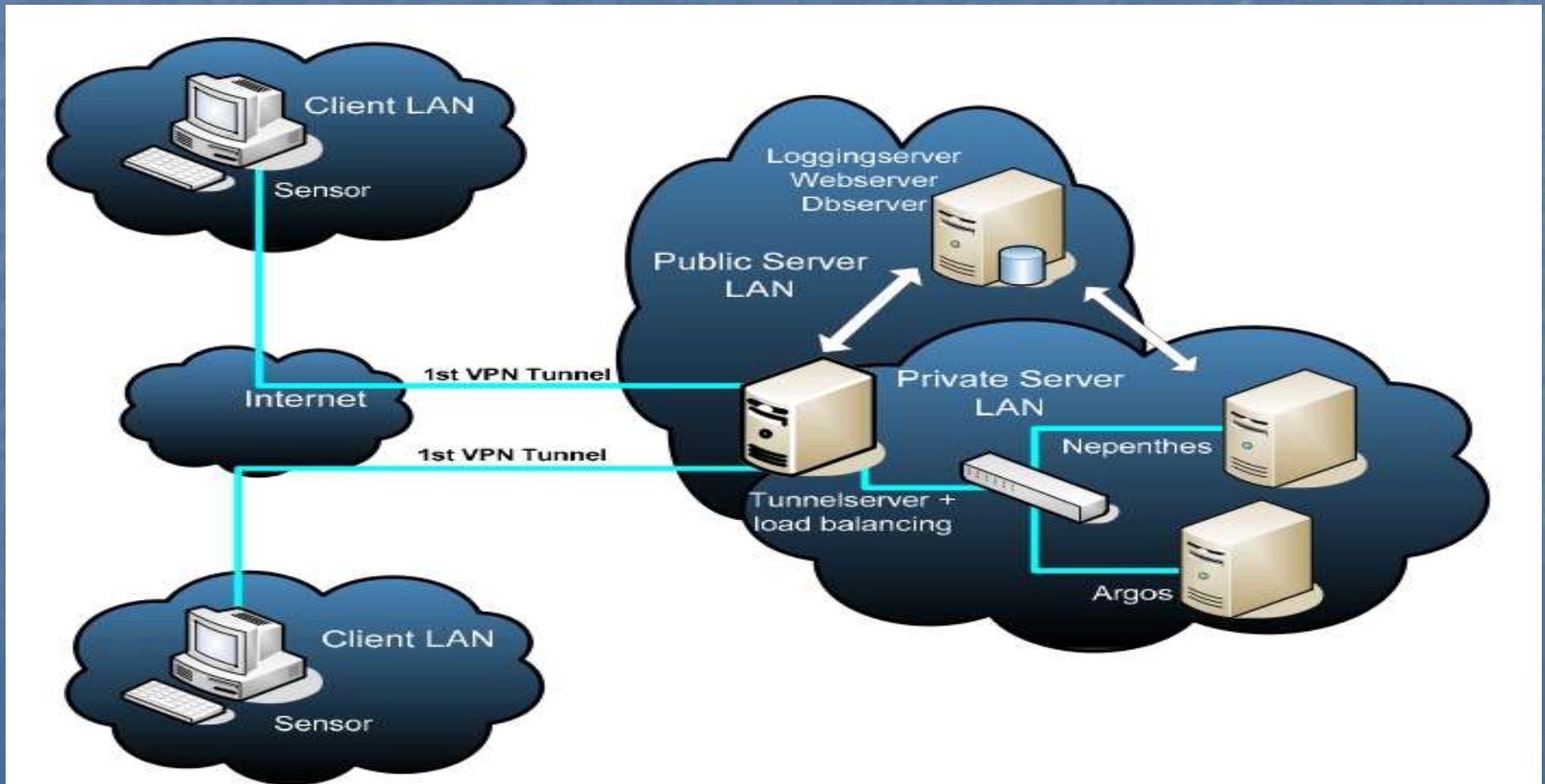


Low Interaction Honeynet System





SURFcert-IDS



Distributed Intrusion Detection System (D-IDS) based on a client-server approach, where the clients (sensors) contain a **honeypot and/or a passive analysis tool like snort.**



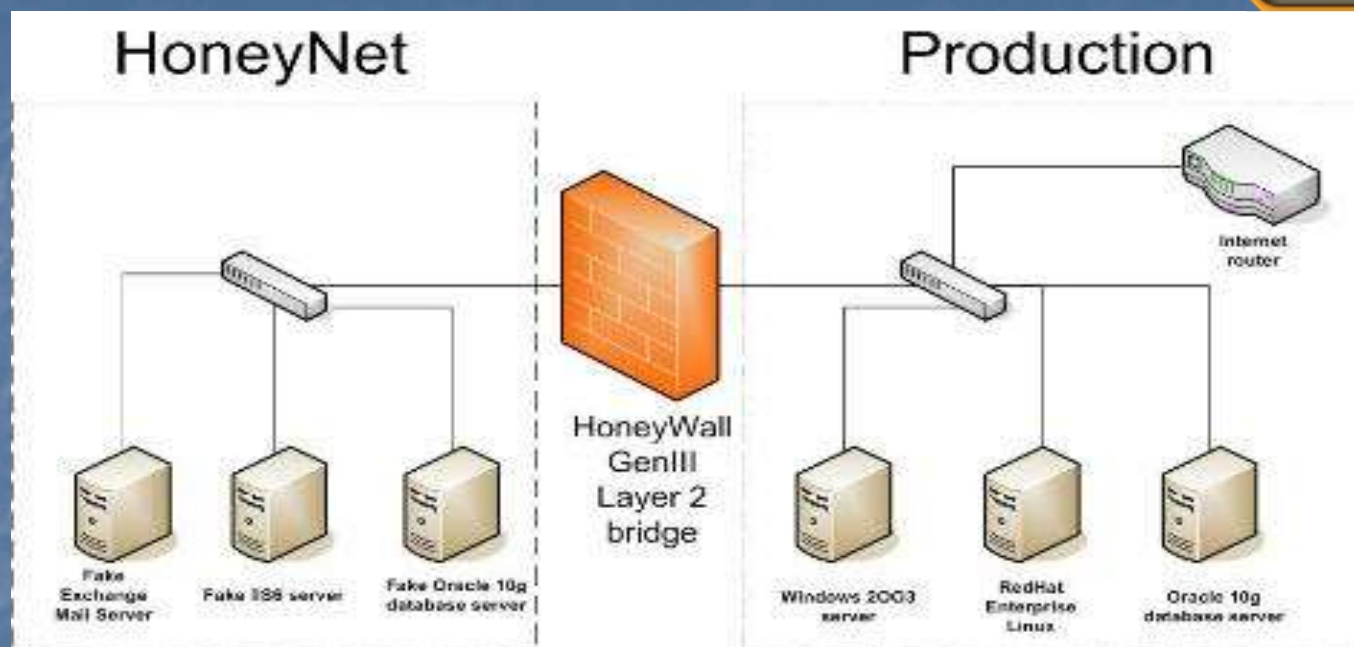
SURFcert-IDS HoneyPot Tools

SMTP-HP		honeypot, which analyze malicious e-mails and use these data in SurfNetids system.
Kippo		a medium interaction SSH honeypot designed to log brute force attacks and, most importantly, the entire shell interaction performed by the attacker.
Dionaea		A low interaction Honeypot, which emulates known vulnerabilities and captures worms as they attempt to infect it.
Glastopf		a Honeypot which emulates thousands of vulnerabilities, to gather data from attacks targeting web applications .

And MUCH MORE



HoneyWall



[HoneyBow](#)

HoneyBow : a high-interaction malware collection toolkit

[Honeymole](#)

used for honeypot farms. Permits to deploy multiple sensors that redirect traffic to a centralized collection of honeypots.

[Honeyd](#) : a honeypot used for capturing attacker activity.

AND Much More



Artifact Analysis
« **Laboratory** »

CUKOO : Open source Malware analysis system.



Execute a Malicious Code (worm, ...) inside environment (SANDBOX)

--> Artifact Analysis Lab

Allow to **understand how artifact operate** and what they would do when deployed

and understand the context, the motivations and the goals of the intruders.

→ response actions

Cuckoo generates :

- Native functions and Windows API calls traces
- Copies of files created and deleted from the filesystem
- Dump of the memory of the selected process
- Full memory dump of the analysis machine
- Screenshots of the desktop during the execution of the malware analysis
- Network dump generated by the machine used for the analysis

[REMnux](#) a freeware , which incorporates many tools for analyzing Windows and Linux malware, like examining browser-based threats (obfuscated JavaScript,..)



[Zero Wine](#) : a full-featured **open-source** tool for dynamically analyzing the behavior of Windows malware by running it in a sandbox (WINE emulator).



The output generated by wine are the **API calls used by the malware**, allowing analysis of malware's behavior

Sandboxie + Buster Sandbox Analyzer : a freeware wrapper around the Sandboxie tool for Windows, which analyze the **behaviour of processes and the changes made to system** and then evaluate if they are malware suspicious



[Malheur](#) a tool for analyzing the volumes of data collected by behavioral sandboxes.

....

Metasploit (community) Framework

Permit to **create and test exploits**, via a modular approach, allowing the **combination of exploits with payloads**

Using the Framework , you are helped in the **steps for exploiting a system**

- Permit choosing and configuring an exploit (more than a thousand of different exploits for Windows, Unix/Linux and Mac OS X) and check whether the intended target system is vulnerable to the chosen exploit
- Choosing and configuring a payload (code that will be executed on the target system upon successful entry)
- Choosing the encoding technique so that the intrusion-prevention system (IPS) ignores the encoded payload;



-III-

**"Implementing" the Information
System of CSIRT services ,**

with Open-Source tools



Incident Handling Process

Incident Tracking System (ITS)



GLPI, Amended version used by TunCERT :originally an Information Resource-Manager (an ITIL compliant Service desk)

- offers very rich functionalities for **Incident Handling Management** and *Technical knowledge sharing*, along with rich statistics and report generation and *ease of amendment of its code*
- *GLPI's main Incident Tracking functionalities*
 - **Tickets (incident Reports)** created manually or by processing of incoming email requests
 - **Tracking of Incident Reports**, with priority management, and possible Link between them (**correlated incidents**) → Concept of “**problems**” (**set of related incidents**)
 - **Assignment of incident**, with display of the interventions assigned to an IH and assignment of time of intervention
 - Handling of requests for validations and **mail tracking of interventions**
 - Management of the **planning of intervention** and display of History of done interventions
 - Management of the tracking of requests, with rules when opening tickets and SLA, with **customizable escalation**

Other Interesting features

- **Knowledge Database** : Management of “know how”, with an FAQ and Content management by targets.
- **Statistics** : Monthly and yearly Global Statistics reports, By **Incident Handler** , **constituency**, **category of incident**, and **priority**.
- **Powerful Search module** (with Bookmark search capabilities)
- **Management of constituency and partner information** with Support of Satisfaction survey handling
- **Confidentiality** : Management of confidentiality of documents
-
- **Reservation** : Management of the reservations for IH tools and equipments, with calendar for reservation
- and much more ...

<http://www.glpi-project.org/>



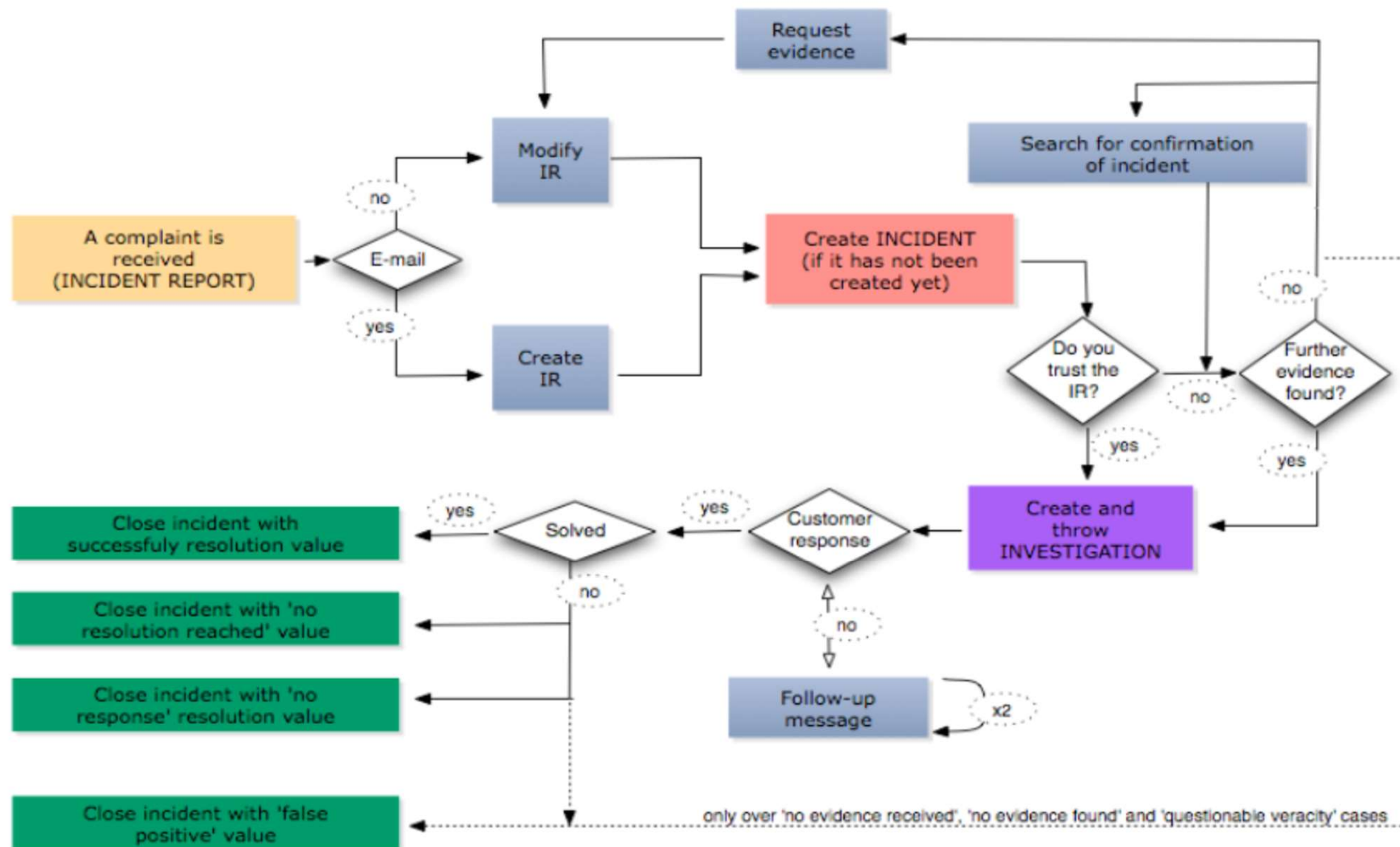
GLPI Tour

Eng Mohamed MABROUK,
TunCERT

Other Open source ITS : RTIR

Incident handling and ticketing open source system, originally developed by JANET CSIRT, And TF-CSIRT

→ Implement the complete **workflow for Incident Handling** management :



Main characteristics of RTIR

- E-mail messages reporting incidents are automatically converted to tickets
- For other reports(phone, fax, memo), you can enter the details into RTIR by creating an **Incident Report** (tickets (incident) can have an SLA or resolution time)
- Permit to check for **correlated events**,
 - Possibility to search inside parts of messages matching regular expressions for IP addresses, hostnames and email addresses.
 - --If the Incident Report involves an issue which is already being dealt with, the Incident Report can be linked to the existing oneS.
- **Concept of Blocking Block** : RTIR permit to create a child ticket of type *Block*,, with information such as the **IP address(es) to be blocked**, **particular services** that are to be blocked, **where the traffic is to be blocked**, details of the affected customer, and the duration that the blocking
- facilities for producing an **Incident Report document & a monthly report** , including all the **statistics** and data required
-

<https://bestpractical.com/download-page>

Ticket Creation via Customer Portal, Email, Phone, Fax

Ticket Management

- Ticket Priorization & Assignment
- Ticket Transmission & Follow-up
- Service Catalog
- Ticket Splitting & Merging
- Ticket Bulk Action
- Ticket Links
- Configurable Ticket Notifications
- Templates

Knowledge Management: FAQ/Knowledge Database/Surveys/
Customer Information Center

Reporting: Generate Statistics with Previews
/CSV/PDF Export/Display in Dashboard

Alert and Warning (& announcement) Process

Easily create your own Security Mailing-list
(+FB, Twiter, SMS, ..)

“The” Tool for the Management of the Alert and Warning Process’s Workflow

Taranis, developed by GOVCERT.NL. specifically designed to fit the workflow of a CSIRT Watch unit, and used by a lot of CSIRTs.

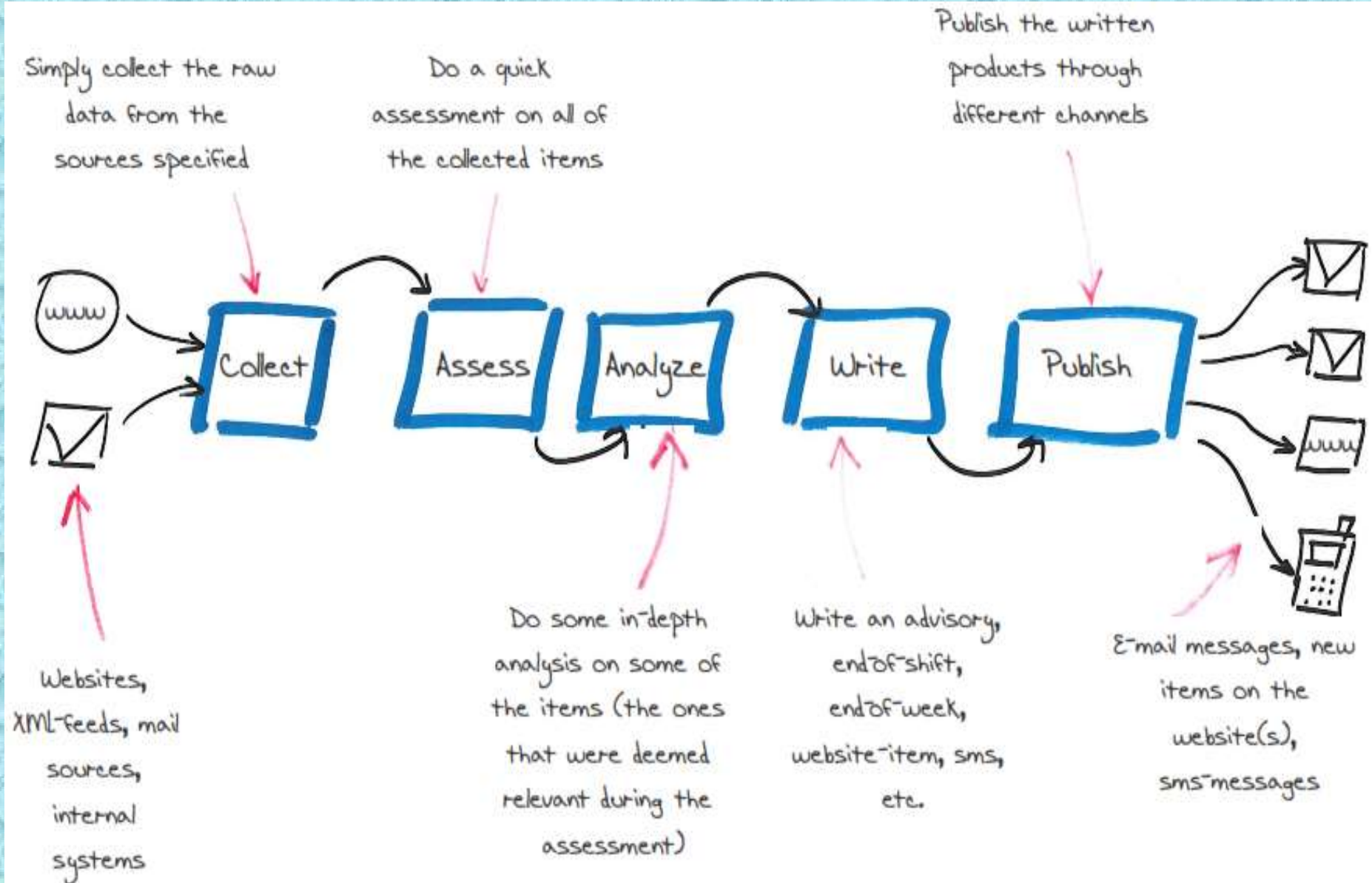
- **implement a workflow for this process** and permit to assist the team in the **collection, analysis and publishing of security information:**
 - **Collect:** Collect information from different sources. Taranis supports around 900 sources: HTTP sources, IMAP and POP3, based sources
 - **Assess:** Determine the relevance of news-items.
 - **Analyze:** Analyze relevant news-items and determine the appropriate products that are to be created on the subject.
 - **Write:** Write **advisories and alert e-mails** and apply the standard quality assurance cycle.
 - **Publish:** Send out the products to the **relevant target audience.**
- Vulnerabilities are directly **indicated with CVE IDs**, and is based on the **CPE Common Platform Enumeration**) list, with mechanisms to keep both lists and the **mapping between them** up to date.



Eng Mohamed MABROUK,
TunCERT



Alerts and Warning Process



SIMPLE Tool for the management of the publishing (NEW CSIRTs)

PHPList : an open-source mailing-list management tool.

Provide interesting features, especially for a **new CSIRT** :

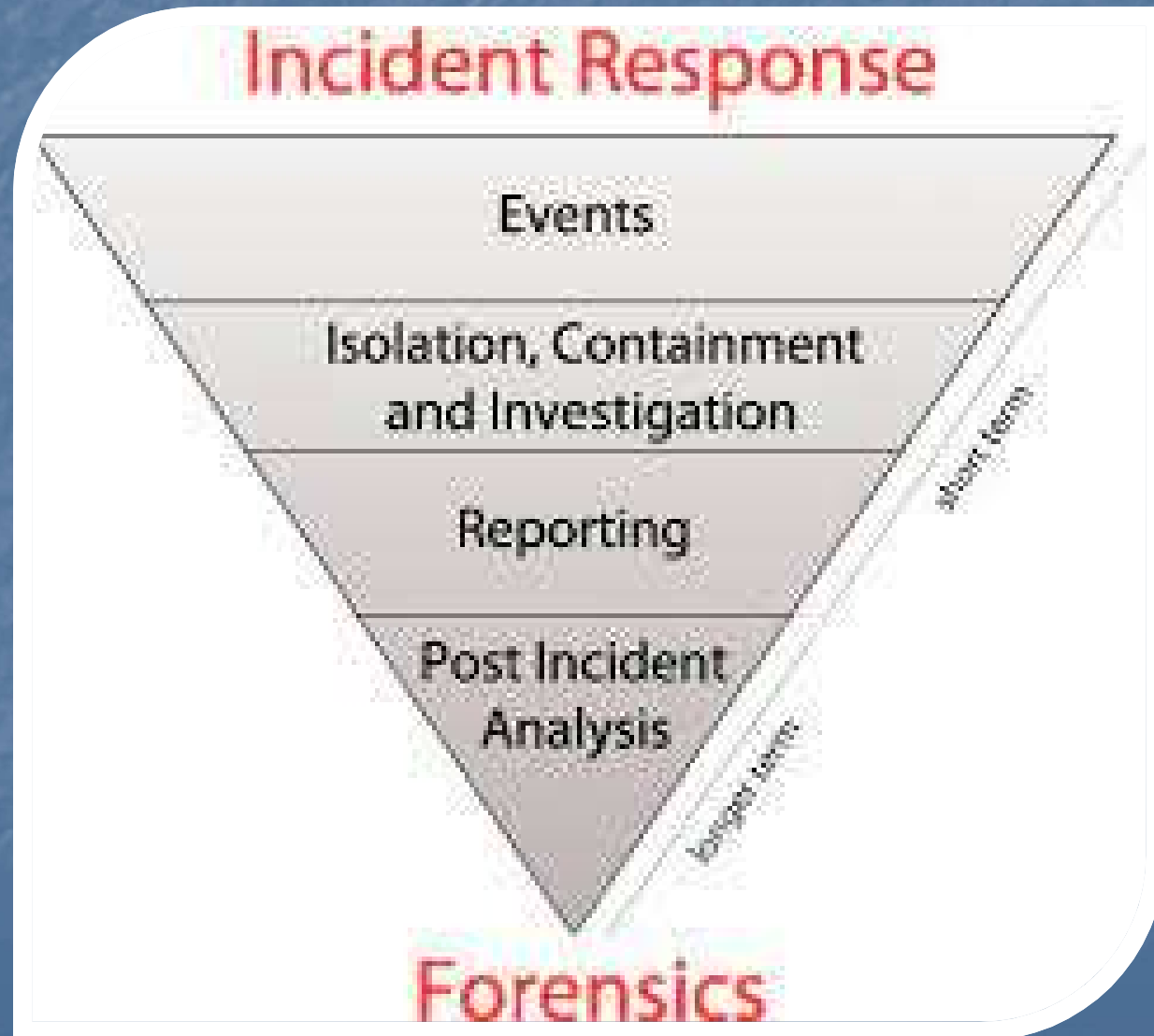
- **Open/View Tracking** : Tells you how many users opened your message.
- **Click Tracking** : tracks links and URLs. Statistics by message, URL and subscriber
- define automated actions on receipt of bounce messages according to matches with regular expressions.
- Batch Sending Processing

....

-III-

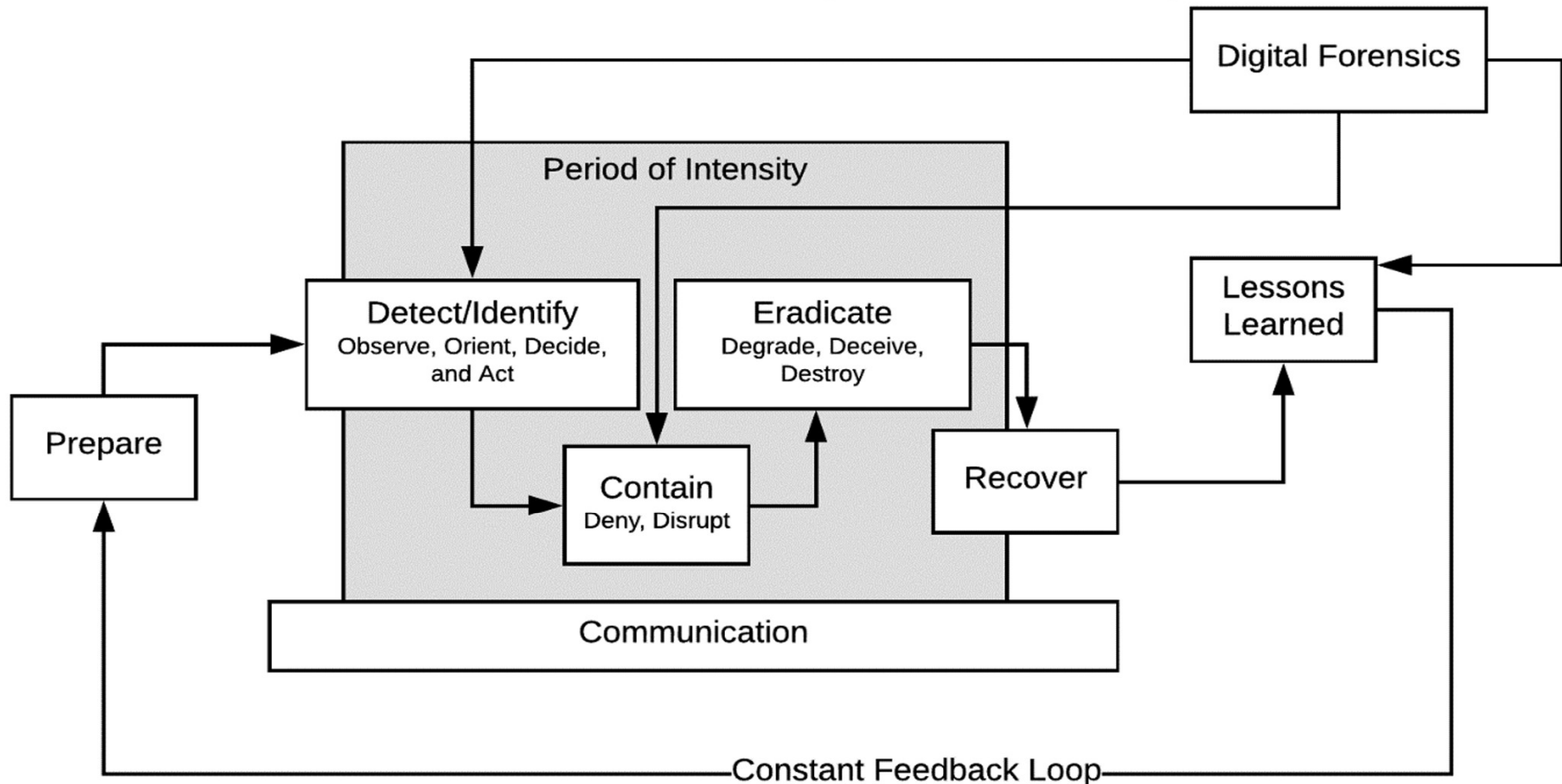
Open-source tools for investigation
and Forensics activities

Incident Response and Forensics



Incident response life cycle

Modern Incident Response Life Cycle



Prepare your artifacts

- Secure Clone
 - FTK Imager
 - DD
- Collect evidences
 - Kape
 - Heoder
 - Autopsy
- Analysing
 - Kuiper
 - APT Hunter
 - Volatility

Prepare your artifact

- Malware analyse
 - Procmon
 - Pestudio
 - Wireshark
 - FakeDNS ...
 - ProcDOT
 - Debugger ollyDBG

Autopsy



→ A **GUI** (available for windows) to the tools available in The **Sleuth Kit**,

→ Provides case management, image integrity, keyword searching, and other automated operations :

- Timeline Analysis - Advanced graphical event viewer interface .
- Hash Filtering - Flag known bad files and ignore known good..

Web Artifacts (extract history, bookmarks, and cookies from Firefox, Chrome, and IE).

Data Carving (Recover deleted files from unallocated space)

Multimedia (eExtract EXIF from pictures and watch videos)

Indicators of Compromise (Scan a computer using STIX).

<http://www.sleuthkit.org/autopsy/download.php>

Sleuth Kit



A **C library** and collection of **command line file forensic tools**.

- Runs on Windows and Unix
- Supports the NTFS, FAT, ExFAT, UFS 1, UFS 2, EXT2FS, EXT3FS, Ext4, HFS, ISO 9660, and YAFFS2 file systems .
- show files that have been **Added /deleted /"hidden"** by **rootkits**
- Analyzes raw , Expert Witness (EnCase) and AFF file system and disk images.

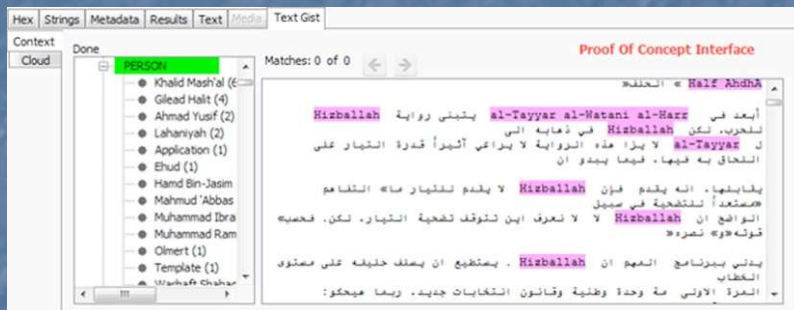
The TSK Framework allows easy incorporation of file analysis modules written by other developers.

Pb : Command Line =>

Adds-on (not free) for Law Enforcement entities :

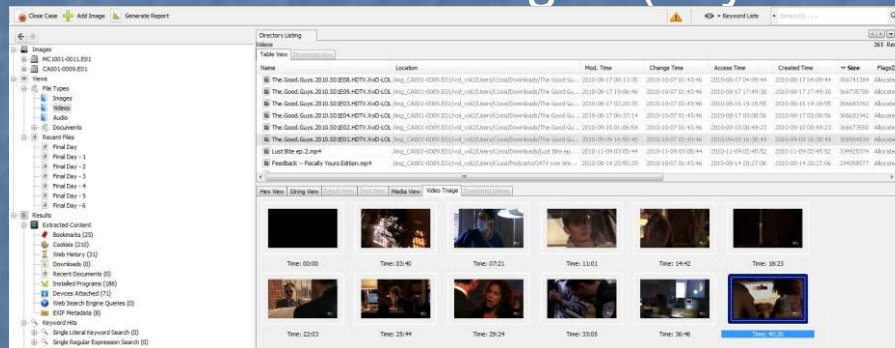
Text Gisting

Analyze foreign-language content on digital media in the field



Video Triage

Efficiently triage video content by splitting video files up into easily viewable thumbnail images (keyframes).



Law Enforcement Bundle

Integrate Project Vic and C4P/All databases to identify known child exploitation images.

Open Source Intelligence (OSINT) Platforms



Maltego

Offer **mining and gathering of information** as well as the representation of this information in a easy to understand format.

- Helps for the **information gathering phase** of all security related work (discovery of "hidden" information).
- Aids in the thinking process, by **visually demonstrating interconnected links between searched items.**

→ Determine the "**hidden**" **relationships** and real world links between:

- Target and Groups of people (social networks)
- Companies & Organizations
- Web sites
- Internet infrastructure (Domains,DNS names,Netblocks,IP addresses)
- Phrases
- Affiliations
- Documents and files

→ provides a GUI that makes seeing these relationships instant and accurate

→ **Highlight hidden connections.**



MISP

- MISIP stands for Malware Information Sharing Platform. It is a Threat sharing platform
- Free and Open Source and exists >10 years
- CIRCL leads development
- Used by >6000 organisations worldwide
- Security teams, national and government CSIRTs, commercial providers

FUNCTIONS OF MISP

- Core functionality is sharing
- Everyone can be a consumer and/ or a contributor/producer
- Quick benefit without the obligation to contribute
- Low barrier to get acquainted to the system

MISP GUI

Home Event Actions Input Filters Global Actions Sync Actions Administration Audit Discussions MISP Admin Log out

List Events

- Add Event
- Import From MISP Export
- List Attributes
- Search Attributes
- View Proposals
- Events with proposals
- Export
- Automation

My Org Filter

Published	Org	Owner Org	Id	Tags	#Attr.	Email	Date	Threat Level	Analysis	Info	Distribution	Actions
✓	CUDESO	ORGRNAME	93	ttp:white	16	admin@admin.test	2016-03-23	Medium	Completed	SAMSAM: THE DOCTOR WILL SEE YOU, AFTER HE PAYS THE RANSOM	All	📄 🗑️
✓	CUDESO	ORGRNAME	91	ttp:white	3	admin@admin.test	2016-03-07	Low	Completed	Ad Serving Platform Used By PUA Also Delivers Magnitude Exploit Kit	All	📄 🗑️
✓	CUDESO	ORGRNAME	92	ttp:white	3	admin@admin.test	2016-03-25	Low	Completed	PETYA Crypto-ransomware Overwrites MBR to Lock Users Out of Their Computers	All	📄 🗑️
✗	CIRCL	ORGRNAME	5	ttp:white Type:OSINT	84	admin@admin.test	2016-02-13	Medium	Completed	OSINT - Turla - Harnessing SSL Certificates Using Infrastructure Chaining	All	📄 🗑️
✗	CIRCL	ORGRNAME	43	ttp:white Type:OSINT	70	admin@admin.test	2016-03-21	Low	Completed	OSINT - STOP SCANNING MY MACRO	All	📄 🗑️
✓	CIRCL	ORGRNAME	10	ttp:white circl:incident-classification="system-compromise"	847	admin@admin.test	2016-03-17	Low	Initial	Potential SpamBots (2016-03-17)	All	📄 🗑️
✓	CIRCL	ORGRNAME	44	ttp:white circl:incident-classification="malware"	290	admin@admin.test	2016-03-17	Low	Initial	Malspam (2016-03-17) - Dridex (122), Locky	All	📄 🗑️
✓	CIRCL	ORGRNAME	16	ttp:white	92	admin@admin.test	2016-03-16	Low	Completed	OSINT - AceDeceiver: First iOS Trojan Exploiting Apple DRM Design Flaws to Infect Any iOS Device	All	📄 🗑️
✓	CUDESO	ORGRNAME	71	ttp:white	25	admin@admin.test	2016-03-11	Low	Completed	PowerSniff Malware Used in Macro-based Attacks	All	📄 🗑️
✓	CIRCL	ORGRNAME	25	malware_classification:malware-category="Ransomware"	32	admin@admin.test	2016-03-16	Low	Initial	Locky (2016-03-16)	All	📄 🗑️

Download: PGP/GPG key Powered by MISP 2.4.28

Open source/Freeware tools for
Digital forensic investigation
(Live DVD distributions)

DFF (Digital Forensic Framework)



Digital file forensic tool and a development platform for digital forensics and evidence gathering.

- *Windows and Linux OS forensics*
- **Preserve digital chain of custody**, by including **Software write blocker**, cryptographic hash calculation and Virtual machine disk reconstruction VmWare (VMDK) compatible
- **volatile memory forensics** (Processes, local files, binary extraction, network connections).
- **Recover hidden and deleted artifacts**(Deleted files / folders, unallocated spaces, carving)
- Read standard digital forensics file formats (Raw, Encase EWF, AFF 3 file formats) and offer Quickly triage and search for (meta-)data, with various tools for Windows and Linux OS forensics (Registry, Mailboxes, NTFS, EXTFS 2/3/4, FAT 12/16/32 file systems).

<http://www.digital-forensic.org/>

A Linux Live CD which bundles some of the most popular open source and freeware) computer forensic tools (**and distributions**) .

Contains **hundreds** of tools for **Mobile Forensics**, Network Forensics, Data Recovery, and Hashing.

DEFT most important package and tool list:

- Full support for Bitlocker encrypted disks
- Sleuthkit , analyze disk images and perform in-depth analysis of file systems
- Mobile Forensics : Full support for Android and iOS logical acquisitions
- File Manager with disk mount's status
- Skype Extractor, utility for reading and extracting information from the Skype Internet telephone software user data files
- open source intelligence tools

<http://www.deftlinux.net/download/>



SANS Institute's Investigative Forensic Toolkit SIFT



VMware appliance, pre-configured with the necessary tools to perform and conduct an in-depth forensic or incident response investigation.

- includes **more than one hundred open-source tools**, including Autopsy, log2timeline for generating a timeline from system logs, Scalpel for data file carving, Rifiuti for examining the recycle bin, and lots more.
- supports analysis of almost all forensics file formats (Expert Witness Format (E01), Advanced Forensic Format (AFF), ..) and RAW (dd) evidence formats.

<http://digital-forensics.sans.org/community/downloads>

CAINE (Computer Aided INvestigative Environment)



CAINE - an (Italian) Linux Live distribution that contains a wealth of digital forensic tools.

Include a **user-friendly GUI**, semi-automated report creation and tools for Mobile Forensics, Network Forensics, Data Recovery and more.

<http://www.caine-live.net/>

- **Windows version** : Win-Ufo , <http://win-ufo.org/>



<http://win-ufo.org/>

A versatile computer forensics environment for **inexperienced** forensic practitioners.

→ Open source forensic/security tools, customized and combined with an **intuitive user interface to create an easy to use forensic environment** :

- Examine physical memory dumps
- Discover USB storage information
- Discover recent documents
- Recover/Carve over 15 different file types
- Examine UserAssist information
- Extract LanMan password hashes
- Get hard disk and partition information
- Extract user and group information
- View Internet histories

And much more :

[Open Computer Forensics Architecture](http://ocfa.sourceforge.net/) OCFA (<http://ocfa.sourceforge.net/>)

...

And also tools for auditing source codes

RATS : tool for scanning C, C++, Perl, PHP, Python and Ruby source code

and flagging common security related programming errors such as buffer overflows and TOCTOU (Time Of Check, Time Of Use) race conditions, ...

Sonar : JAVA

Seven analysis axis, with potential bugs detection :

+ Plugins for C, C#, PHP, PL/SQL, also Cobol ...

FindBugs, for Java

Other code source checkers, for C :

C++ lint: <http://sourceforge.net/projects/clint/>

flawfinder, : <http://www.dwheeler.com/flawfinder/>

PScan: <http://www.striker.ottawa.on.ca/~aland/pscan/>

Splint : <http://splint.org/>

Cqual : <http://www.cs.berkeley.edu/~jfoster/cqual/>

MOPS : <http://www.cs.berkeley.edu/~daw/mops/>

BOON <http://www.cs.berkeley.edu/~daw/boon/>

Blast : <http://www-cad.eecs.berkeley.edu/~rupak/blast/>

LCLint: <http://lclint.cs.virginia.edu/>

ITs4: <http://www.cigital.com/its4/>



HANDS ON



- CSIRT.TN KIT (FTK, Autopsy, KAPE ...)
- REM Windows
- REM Linux
- Kuiper Framework

Start Small, and increment
gradually

Skills FIRST!!!

« A word » on equipments
for IH team

• **Special Local Infrastructure**

This team will have at his disposition:

- A physically disconnected network, that it should manage by its own staff.
- One medium-size server, which will be used for :
 - supporting incident handling tools and activities
 - hosting the Incident tracking system (incident follows-up) used by this team
 - Local back-up and archiving.

This server will be only accessible from the disconnected physical network of the IH team. + Protected ponctual physical connections can be provided for the CSIRT manager, and monitoring center operators in charge of Incident report feeding into the “ticketing system”. Strong authentication methods should be applied for those access (One-time passwords tokens, and waiting for that, starting by a VPN solution (SSH)).

You should keep this physical separation, while providing separate workstations for the team, to access the internal IS, Internet and other services offered by the main servers (bulk-archiving, ..), or via secure double NIC and boots.

➤ you will foresee, when you will have the necessary well skilled IT staff, to study how to establish very secure ponctual connections to the rest of the network (automatic access to the main server (for bulk-archiving, access to

Laboratory-Room for Mobile devices forensics (Mobile phones, Tablets, GPS devices, ...)

For the collection of mobile devices :

RF shield bag (prices Varies from 50 to 200 \$): a bag you can place a cell phone, 3G-tablets into, so that it cannot receive any signals. This prevents changes from taking place in the phone due to receiving a signal or tries of “owners” to erase remotely their content.

Arson Cans, that are available through local fire departments. If not available, empty paint cans can be used with less reliability, until sell of arson cans.

These bags are not perfect. Consider wrapping the device in three layers of aluminum foil and then placing it in the bag or an arson can.

For the analysis of the mobile devices, you should provide all necessary little hardware tools (SIM readers, connectors, chargers , ...) and electronic directories about portable devices, which permits to identify the manufacturer and model, if the device is destroyed partially or damaged.

*Email of tunCERT and CSIRT.tn
Trainers, in charge of Demos*

TunCERT :

Eng Mohamed Ben MABROUK : benmabrouk.medali@ansi.tn
GLPI, Taranis,

Eng Mondher SMII : smii.mondher@ansi.tn
Pfsense, Surricata ,Oignon, Saher

CSIRT.tn :

Eng Amine RACHED : amine.rached@keystone.tn
CSIRT.TN KIT (FTK, Autopsy, KAPE ...), REM , Kuiper Framework)

That's All Folks
THANK YOU VERY MUCH FOR
YOUR ATTENTION

- ***For inscriptions to the Live Platform or/and Download of Live-DVD : Please send an email to : events@ansi.tn with CC nabilsahli@gmail.com (/n.sahli@ansi.tn) for follows-up***
- ***For inscriptions to Additional Trainings (Installation/Configurations): Please send an email to : events@ansi.tn (with CC nabilsahli@gmail.com), specifying the Tool(s) you are interested with***